Seventh Workshop on the Economics of Information Security,
Center for Digital Strategies, Tuck School of Business,
Dartmouth College, Hanover, NH, June 25-28, 2008.

Do Data Breach Disclosure Laws Reduce Identity Theft?

Sasha Romanosky, Rahul Telang, Alessandro Acquisti
Heinz School of Public Policy and Management, Carnegie Mellon University
{sromanos, rtelang, acquisti}@andrew.cmu.edu

ABSTRACT[1]

Identity theft resulted in corporate and consumer losses of $56 billion dollars in 2005, with about 30% of known identity thefts caused by corporate data breaches. Many US states have responded by adopting data breach disclosure laws that require firms to notify consumers if their personal information has been lost or stolen. While the laws are expected to reduce losses, their full effects have yet to be empirically measured. We use panel from the US Federal Trade Commission with state and time fixed-effects regression to estimate the impact of data breach disclosure laws on identity theft over the years 2002 to 2006. We find no statistically significant effect that laws reduce identity theft, even after considering income, urbanization, strictness of law and interstate commerce. If the probability of becoming a victim conditional on a data breach is very small, then the law's maximum effectiveness is inherently limited. Quality of data and the possibility of reporting bias also make proper identification difficult. However, we appreciate that these laws may have other benefits such as reducing a victim's average losses and improving a firm's security and operational practices.

Keywords

Data breach legislation, security breach, information economics, identity theft, fraud, fixed-effects regression

1. INTRODUCTION

Consumer identity theft resulted in corporate and consumer losses of around $56 billion dollars[2] in 2005 with about 30% of known identity thefts caused by corporate data breaches (Javelin Strategy & Research, 2006). A data breach occurs when personally identifiable information such as name and social security or credit card number is accidentally lost or maliciously stolen. These breaches can result in hundreds of thousands (sometimes millions) of lost records, leading to identity theft and related crimes. In an effort to reduce these crimes, many US states have responded by adopting data breach disclosure laws that require firms to notify individuals when their personal information has been compromised.

1.1 Support for data breach disclosure laws

The spirit of the data breach notification laws are contained within two phrases: "*Sunlight as a disinfectant*,"[3] and "*Right to know*." First, by highlighting a firm's poor security controls, legislators hope to create an incentive for all firms (even those that have not been breached) to improve their controls thereby "disinfecting" themselves of shoddy security practices (Ranger, 2007). Notification can "transform [private] information about firm practices into publicly-known information as well as alter practices within the firm" (Schwartz and Janger, 2007). Proponents believe that the laws will force firms to internalize more of the cost of a breach through notification letters, customer support call centers, and mitigating actions such as marketing campaigns and free credit monitoring.

---

[1] Please note this is a working paper. Please contact Sasha Romanosky for the most current version.

[2] This value was calculated as the estimated number of identity theft victims in 2005 multiplied by the average amount stolen per victim: 8.9M victims * $6,383 loss/victim = $56.6B. (Actual amount lost per consumer was $422 on average.)

[3] This phrase is originally attributed to Justice Louis Brandeis, 1933, http://www.brandeis.edu/investigate/sunlight/, accessed 11/08/07.

Second, this form of light-handed paternalism often represents a preferred approach to legislative enforcement compared with a "command and control" regime (Magat and Viscusi, 1992). Consumers feel that they have the right to be informed when firms, *use* or *abuse* their information. Having being notified of a breach of their personal information, consumers could then make informed decisions and take appropriate actions to prevent identity theft. For example, to mitigate the risks, consumers can alert their bank, credit card merchant, the FTC, or law enforcement. They can close unused financial accounts, or place a credit freeze or fraud alert on their credit report.[4] Notifications can also enable law enforcement, researchers, and policy makers to better understand which firms and sectors are best (worst) at protecting consumer (and employee) data. Ponemon (2005) showed that consumers lose confidence in firms who suffer breaches. Though, it may only be through legislation that firms acquire enough incentive to actually improve their practices to reduce the likelihood of future breaches and repair consumer confidence.

Moreover, at least four US congressional hearings have convened to discuss how data breach laws may reduce identity theft (US Congress, 2005a, 2005b, 2005c, 2005d). The connection has even warranted a special report from the US Government Accountability Office (GAO) examining the effect of data breach disclosure laws on identity theft, yet their findings have been inconclusive (Wood, 2007). Californian legislators consider their data breach law as a possible remedy for identity theft:[5] "This bill is intended to help consumers protect their financial security by requiring that state agencies and businesses that keep consumers' personal information in a computerized data system to quickly disclose to consumers any breach of the security of the system, if the information disclosed could be used to commit identity theft." Further, the UK Science and Technology Committee claims that, "data security breach notification law would be among the most important advances that the United Kingdom could make in promoting personal internet security" (House of Lords, Science and Technology Committee, 2007).

1.2 Arguments against data breach disclosure laws

However, it is unclear whether this kind of disclosure regime does, in fact, produce a socially optimal outcome. While it may improve a firm's security practices and allow consumers to mitigate the risks of identity theft, some claim that it may also create unnecessary costs for firms and consumers, lowering social welfare and reducing innovation and ecommerce activity. Lenard and Rubin (2005, 2006), for example, argue that if, indeed, the probability of a consumer suffering identity theft is low enough, then both firms and consumers could incur unnecessary costs by overreacting. Firms would incur the unnecessary costs of notifying consumers, and consumers would incur the unnecessary costs from constantly freezing and thawing their credit reports. Second, they argue that these policies impede e-commerce and stifle technological development by discouraging firms to innovate using consumers' personal information (or stop collecting it altogether[6]). They also consider how firms are burdened by complying with multiple, disparate, and perhaps conflicting disclosure laws. They further conclude that these laws are unnecessary because of the following:

- The probability of becoming a victim to identity theft as a result of a data breach is very low, around only 2%.
- The externality is not as severe as claimed because around 90%[7] of the cost of identity theft and fraud is already born by the firms (businesses, banks, credit card issuers, merchants).
- Firms may use self-regulated notifications as a market differentiator. If sufficiently valued by the consumer, the market will react accordingly, favoring those firms who choose to disclose.
- The notices, themselves, may go unheeded either if no one reacts to the warning, or if consumers receive too many notices, desensitizing or confusing them about the risk.

An article in the Wall Street Journal "Business Technology Blog" agrees that something must be done to prevent future breaches, but disagrees that the solution lies with government legislation. It argues that because of the speed by which online attacks change, more legislation would simply produce a lowest threshold of compliance, "Our biggest fear is that legislation will result in worse security by giving companies a security floor to meet that's fine for 2007 but will feel helplessly outdated

[4] A fraud alert informs potential creditors that a consumer may have been a victim of identity theft. The creditor must then take additional measures to verify the identity of the consumer. A credit freeze prevents a creditor from checking a consumer's credit report, or opening new accounts.

[5] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html, accessed 10/05/08.

[6] Of course, information security practitioners and proponents of the law would argue that this is, in fact a beneficial outcome.

[7] As estimated by Javelin Research in 2003 (90.5%), 2005 (89.6%) and 2006 (93.7%)

a few years from now."[8] Moreover, they claim that the policies will become, "[a] set of rules that companies spend money complying with, but which doesn't end up preventing the crimes it was designed to stop."

1.3 Summary

These arguments present a stimulating debate as to whether data breach disclosure laws reduce identity theft, and something which, to our knowledge, no one has attempted to empirically measure. Using panel data on identity theft gathered from the Federal Trade Commission (FTC) over the years 2002 to 2006, we use state and year fixed effect regression analysis to empirically estimate the impact of data breach laws on the frequency of identity thefts.

We find no statistically significant effect that laws reduce identity theft, even after considering income, urbanization, strictness of law and interstate commerce. The lack of a significant negative effect may be due to breaches accounting for a small enough percentage of total identity thefts, dwarfing any actual crime reduction by more common causes such as lost or stolen wallet. Quality of data and the possibility of reporting bias also make proper identification difficult.

The rest of the paper is organized as follows: Section 2 provides background literature on various forms of information economics and disclosure policy. Section 3 describes the causes and characteristics of data breaches and data breach legislation. Section 4 describes the sources of identity theft and summary statistics. We perform data analysis in Section 5 and discuss policy implications in Section 6.

2. RELATED WORK

2.1 Information Economics and Disclosure Policy

A policy maker considers losses by both consumers and firms when determining the optimal level of disclosure legislation. Consider a firm deciding whether to disclose or conceal information about the quality of its product or service to their customers, law enforcement or government agency. While incentives exist for firms to voluntarily disclose favorable information, they clearly prefer to conceal unfavorable information. Firms realize that the cost from disclosure increases the more they internalize (or are liable for) consumer losses. However, social welfare may increase when the consumer takes measures to mitigate their risk of harm.

Many researchers have studied variations of this scenario. For example, Shavell (1987) examines the incentives for producers to reveal favorable information, and the rewards to firms that conceal unfavorable information. He shows how sellers with low quality goods conceal information about their products and free ride off of competitors with better quality goods. i.e. "parties with verifiable information less favorable than a certain threshold will keep silent." He presents an example of a car dealership with information on the mechanical problems for the cars. They will likely not disclose even minor problems because the sale price of used cars will increase from sellers of unverifiably higher quality cars.

Polinsky and Shavell (2006) examine how firms acquire information about their products in mandatory and voluntary disclosure policies. They note that mandatory disclosure is better for the consumer, but that in conjunction with a liability regime, can also lead to a suboptimal outcome because it "reduces incentives for firms to acquire information about product risks in the first place (through research, product testing)."

Mathios (2000) examines the effect of mandatory disclosure of food labels on salad dressings in a chain of New York grocery stores. He discusses how market incentive can exist for firms to disclose product information. Namely: if consumers know the value of products, if firms have credible methods of communicating quality, and where consumers are skeptical when firms don't disclose product information. He describes other models that predict how voluntary disclosure leads to "partial unraveling of information." For instance, that firms don't voluntarily disclose when it's costly, or when they can't credibly "convey the information."

Jin and Leslie (2003) study health information disclosure in the restaurant industry. Specifically, they find that disclosing the hygiene quality of a restaurant increases health inspection scores. Moreover, and importantly, this became a credible signal to consumers who responded by demanding cleaner restaurants.

Arora, Telang and Xu (2004) discuss the role of a policy maker in the optimal time to disclose software vulnerabilities. Here, the competing forces are the costs to the firm to develop, test and release a patch for the affected software, versus the cost the consumers would incur in the event of an attack that exploits that vulnerability. Costs to the firm decrease with time, and costs to the consumer are increasing with time (more attacks over time). They find that software vendors wait longer than is socially optimal to release a patch and that neither instant disclosure nor non-disclosure is optimal.

[8] http://blogs.wsj.com/biztech/2007/10/11/congress-moves-on-data-security/, accessed 02/13/08.

Magat and Viscusi (1992) argue that disclosure legislation will only be effective if the human element is considered. That is, disclosure will be more successful when the warning provides relevant information that helps the user make an informed decision. They claim that, "consumers do not always respond rationally to both the information and the changes in risk levels. To be effective, information programs must convey information in a form that can be easily processed, and in an accurate and meaningful way that will enable individuals to make informed decisions."

Together, these studies discuss the incentives for firms to disclose information about the quality of their product or service and how this changes under different liability regimes.

2.2 Environmental Disclosure and Deterrent Policies

There is a strong precedent of disclosure legislation in the United States. For example, the Food and Drug Administration (FDA) requires that a firm notify them if it encounters, "any adverse experience associated with the use of the drug that is both serious and unexpected," or if "any finding from tests in laboratory animals that suggests a significant risk for human subjects."[9] The Federal Hazardous Substances Act "requires precautionary labeling on the immediate container of hazardous household products to help consumers safely store and use those products and to give them information about immediate first aid."[10]

The Environmental Protection Agency (EPA) requires that, "if a release of an extremely hazardous substance occurs...the owner or operator of the facility shall immediately provide notice…to the community emergency coordinator."[11] A specific example of their efforts is the Toxic Release Inventory (TRI) program developed by the Environmental Protection Community Right to Know Act (EPCRA).[12] Firms polluting above a certain threshold must report the quantity and type to the Environmental Protection Agency. Hamilton (1995) discovered that the first disclosure reduced firm stock price by 0.3%, or a loss of $4.1M in stock value on the day of the disclosure. Konar and Cohen (1997) found that after announcement of TRI, firms with the largest negative (abnormal) stock returns reduced their emissions the most. These studies support the "sunshine" law effect - that firms do respond to such policies by improving their practices.

Cohen (2000) states that, "information disclosure about law violations might be another form of penalty in addition to any direct government-imposed monetary fine." He lists a number of reasons why information disclosure about a firm's environmental penalty would be relevant to shareholders:

- The dollar value may impact the expected value of the firm (valuation of stock price)
- It would be a cause of concern for lenders not wanting to lend to risky firms
- Ancillary penalties such as sanctions from innovation or expansion
- Lost sales from "green" consumers

Cohen studied alternative environmental deterrence policies on environmental disasters. Specifically, he examines empirical studies that estimated the effects of monitoring (inspections) and enforcement (civil suits, criminal penalties, and fines) activities on firms. In the context of oil transport operations and pulp and paper mills, he states that, "studies show that both increased government monitoring and increased enforcement activities result in reduced pollution and/or increased compliance." Further, he describes regulations that impose a fine on the firm for an employee's negligent or malicious activities, and observes that when the fine is too high it creates a perverse incentive for the firm not to monitor its employees. If the fine is too low, of course, the firm has little incentive to comply with enforcement. The implication for this paper is that if the penalty of disclosing a breach is too high, it may reduce a firm's incentive to install appropriate security tools to detect a breach.

Many of the empirical studies of environmental incidents involve coast guard monitoring of oil spills and paper and pulp mills. For example, Epple and Vischer (1994) examined coast guard monitoring of oil transfer operations. They found that a 10% increase in monitoring reduced spill volume by 3.1% but increased spill frequency by 2.1%. That is, they found a significant deterrent effect (by reduced incident severity) but an increased detection of violations. Cohen (1987) examined the impact of targeted and random monitoring of oil transfers and found that targeted monitoring reduced spill volume by 1.7%, and random monitoring reduced spill volume by 2.0%.

---

[9] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=312.32, accessed 10/28/07.

[10] http://www.cpsc.gov/businfo/regsumfhsa.pdf, accessed 10/28/07.

[11] http://www.epa.gov/region5/defs/html/epcra.htm, accessed 10/28/07.

[12] http://www.epa.gov/tri/whatis.htm, accessed 02/13/08.

These studies demonstrate a long history of disclosure legislation as applied to the environmental sector. They show that forcing firms to disclose harmful outcomes can provide a deterrent effect through proper enforcement as a function of inspection and monitoring.

2.3 Criminal Deterrence Policies

Data breach notification laws, as with many environmental or criminal laws are, in essence, deterrent policies. Whether enacted to reduce pollution, street crime, or adjust a firm's incentives, there are generally three methods by which deterrent policies can be effective: increasing the perceived probability of conviction (certainty), increasing the harshness of punishment (severity), or accelerating the swiftness of punishment (celerity) (Akers and Sellers 2004). Certainty would represent the likelihood that a firm (its customers, or others) detects a breach. Severity would represent the cost of the breach to the firm as a function of consumer redress, civil lawsuits, fines, fees, etc.. Celerity would represent the time from when information was lost or stolen until the firm became aware of it.

Many criminologists have studied deterrence effects of law, in general (Clonginger 1975; Blumstein et al, 1978; Levitt 1995; Nagin 1998; Robinson, Darley and John, 2003) and others have focused specifically on the deterrent effects of gun laws and crime (Lott and Mustard 1997; Black and Nagin 1996, Donohue and Ayres 2003) and capital punishment (Mocan and Gittings 2003; Donohue and Wolfers, 2006). While there appears to be no conclusive evidence to overwhelmingly support deterrence policies, for the purpose of this study, we gain valuable insight into methodological approaches of crime research.

3. DATA BREACHES AND BREACH LEGISLATION

3.1 Data Breaches

A data breach is generally considered an "unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information"[13] Types of sensitive and personal information include name, date of birth, social security number, passport ID, driver's license, biometric, or any other kind of personally identifiable, government-issued, medical, or tax information. Sources of data breaches are presented below in Table 1.[14] The data represent 773 breaches of US organizations collected by Attrition.org from the years 2002 to 2007.

Table 1 : Summary Statstics of soures of data breaches

Business Type	Count	Percentage	Total Records Lost	Average No. of Records Lost
Business	246	32%	209M	850k
Educational	246	32%	6M	24k
Government	201	26%	47M	233k
Medical	80	10%	5M	63k
Total	773	100%	267M	

Educational institutions and businesses incur about the same percentage of breaches (~32%), but private sector firms are by far responsible for the greatest average number of records lost (850k per breach). Of the 773 breaches, 190 were a result of internal (42 malicious and 146 accidental) activities, 575 were caused by external sources (hackers, etc), and 8 were unknown. 600 involved theft of social security numbers, and 63 involved credit card numbers. 72 were due to lost data and 35 were due to errors with disposal of data.

There are a number of ways that firms become aware of a breach. First, they may detect the breach themselves, either when an IT or security staff notices unauthorized access to sensitive information, or suspicious transmission of data. They may be notified by a customer or concerned citizen who notices that personal information has suddenly become publicly available. They may be informed by a customer who notices suspicious activity on a financial statement or credit report and contacts the firm directly. According to a 2007 survey of 702 firms, 42% of breaches occur because of lost or stolen hardware (laptops, PDAs, portable memory devices) (Ponemon, 2007).

[13] http://www.dccouncil.washington.dc.us/images/00001/20061218135855.pdf, accessed 10/04/07.

[14] http://attrition.org/dataloss/dataloss.csv, last accessed 08/22/07.

3.2 US Data Breach Disclosure Legislation

As of December 31, 2006, 28 US states had adopted data breach legislation, as shown in Figure 1.[15]

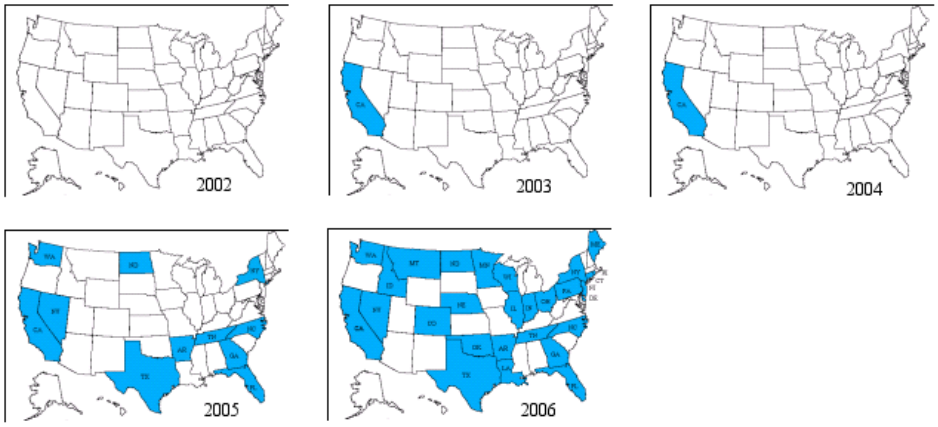


Figure 1: Adoption of breach notification laws from 2002-2006

While details of the legislations vary across states, their central themes are consistent. Specifically, they require notification a) in a timely manner, b) if personally identifiable information c) has either been lost, or is likely to be acquired, by an unauthorized person, c) and is reasonably considered to compromise the confidentiality, integrity or availability of the individual. Specifically, all of the laws address the following topics:

Definition of a Breach: The state laws are generally consistent in regard to what constitutes a data (or security) breach. For instance, the California law, SB. 1386 defines a breach as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." (Hutchins, 2007). Whereas, Nebraska describe a breach as "unauthorized access of unencrypted computerized data that compromises the confidentiality, integrity or availability of personally identifiable information maintained by an individual or commercial entity."[16] Some state laws such as in California, New York and Arkansas account for data on paper, rather than just digital information.

Personally Identifiable Information (PII): Generally, PII includes part of a consumer's name in addition to another piece of identifiable information. For example, the California law describes PII as, "individual's first name, or last name and first initial, in combination with a social security number, driver's license or other state identification card number, or account number, credit or debit card number with the necessary access code or password." Kansas relaxes the requirement for the access code or password, whereas other states expand the definition. Arkansas and Delaware, for example, include medical information, and Nebraska, North Carolina and Wisconsin include biometric data.

Trigger: A critical differentiator of the state laws is the trigger, or threshold, by which notification must be made. 17 states require notification when the personal information is reasonably assumed to have been acquired by an unauthorized party. Whereas, the others require notification only if it is reasonable to believe the information will cause harm to consumers. That is, whether the information has been lost or stolen (acquisition-based, lower threshold), or whether there is reason to believe the information could be used maliciously (risk-based, higher threshold).

Covered Entities: State data breach laws do not apply to all public and private agencies homogenously. For example, both Maine's and Georgia's laws apply to data brokers only, as opposed to private firms or government agencies. That is, "a person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes." The specificity of Georgia's law is likely due to the fact that Choicepoint, the data broker that suffered the very popular data breach, is headquartered in Georgia. 23 state laws apply to all categories, private-sector firms, data brokers and state agencies, whereas 13 apply to only 2 of the 3 categories.

---

[15] For the purpose of this paper, we are including the District of Columbia, but not city-specific breach laws such as in New York city.

[16] http://www.das.state.ne.us/nis/greports/bug/LB_876.pdf, accessed 02/18/08.

Notification: Notification refers to the timeliness by which the firm must notify the consumer. It also describes to whom notifications must be sent. For example, the consumer, law enforcement, state agency, and/or congress. The method of notification is also described (by phone, email, fax) but alternative channels are available if the cost of notification exceeds a stated dollar value, or the number of compromised accounts is greater than a certain threshold, or the firm does not have sufficient contact information. For example, the California law allows for substitute notification if the cost exceeds $250,000 or if the number of affected consumers exceeds 500,000.

Exemption (Safe Harbor): Some state laws provide exemption for firms already governed by industry-specific legislation. For example, 16 states including Indiana, Michigan and Minnesota provide exemption for financial firms if they are governed by GLBA. 7 states including Arizona, Hawaii and Indiana provide exemption for firms governed by HIPAA. Other exemptions are provided if: the firm has contacted law enforcement and they believe consumer notification may jeopardize the investigation; if the data has been encrypted (although many laws do not specifically define this); if the compromised data exists in paper form only; if the number of consumers affected is below a certain threshold; or if the data are public to begin with.

Penalties: The consequences of not complying include state attorney general and civil right of action. Many states do not specify a maximum civil penalty, but some do. For example, the Arizona and Arkansas laws allow a civil penalty not exceeding $10,000, whereas the limit is $25,000 in Connecticut and Idaho, but $500,000 in Florida.

An important characteristic of these state laws is that the residency of the consumer rather than the location of the breach drives disclosure. Therefore, a firm that incurs a data breach must comply with the state laws of each of their affected consumers. For example, if a retail firm in Oregon incurs a breach, it must notify any consumer that resides in California. However, if one of these consumers reports identity theft to the FTC, it may be counted as a report from California, not Oregon. The consequence of this is that when California adopted the law in 2003, firms located across the United States were affected. It was, in fact, because of California's law that Choicepoint was forced to notify Californian residents, even though the company is headquartered near Atlanta, Georgia.

4. IDENTITY THEFT AND THE FTC

4.1 Causes of Identity Theft

Most often, the causes of identity theft is not known, but is an important consideration when estimating the maximum potential effect of data breach disclosure laws. Realistically, the laws would not reduce identity thefts due to stolen mail or garbage. However, identity thefts that fall within a firm's control *could* be reduced by such laws. In a randomized phone survey conducted by Synovate (on behalf of the FTC, 2007), 12% of identity thefts occurred as a result of interaction with firms, while another 56% of victims did not know the cause. This places an approximate bound on the potential effect from 12% to 68% (12% + 56%). In another survey of 505 victims conducted by Javelin Research (2006), 16%[17] reportedly fell within the control of businesses. Researchers at the Center for Identity Management and Information Protection (CIMIP) at Utica College studied 517 identity theft cases from the US Secret Service (2007). In the 274 cases (53%) where the source could be determined, 26.5% originated from firms. A comparison of these causes is shown below in Table 2.

Table 2: Causes of Identity Theft

Cause	Synovate (2007)	Javelin (2006)	CIMIP (2007)
Unknown	56%	53%	47%
Company Controlled	**12%**	**16%**	**26.5%**
Lost/Stolen Wallet	5%	14%	6.2%
Personally knew thief	16%	7%	8.3%
Lost/stolen mail	2%	4%	4.6%
Computer/Phishing/Internet	2%	4%	3.3%
Other	7%	2%	4.1%
Total	100%	100%	100%

Once appropriated, attackers use personal information in many ways. For example they can incur fraudulent charges on existing accounts, or apply for new utilities (phone, electrical, television, internet) and financial accounts such as credit cards,

[17] The data have been rescaled to account for the 270 individuals who did not know of the source of identity theft. The categories controlled by the firm are: Taken by a corrupt business employee: 15%, Some other way: 7%, Misuse of data from an in-store/onsite/mail/telephone transaction: 7%, Stolen from a company that handles your financial data: 6%.

mortgages, and loans (Givens, 2000). They can appropriate a victim's social security number, driver's license or passport to obtain identification or medical benefits. The CIMIP study (2007) of 517 Secret Service identity theft cases revealed that 78% of criminals used the victim's identity to obtain and use credit or cash, 22.7% used the identity to conceal their own identity, and 20.9% applied for vehicle loans.

4.2 Data Sources and Summary Statistics

Surveys can be useful tools for gathering data on actual crimes. For example, the Bureau of Justice Statistics, as part of the National Crime Victimization Survey, conducts phone interviews of around 49,000 households asking whether anyone in the household has been a victim of any number of crimes, including identity theft. The interviews were conducted from July to December in 2004 and January to December in 2005. Identity theft was defined as: "unauthorized use or attempted use of existing credit cards, unauthorized use or attempted use of other existing accounts such as checking accounts, or misuse of personal information to obtain new accounts or loans, or to commit other crimes." Their surveys found approximately 7.2 million victim households (3.3%) in 2004 and 6.4 million victim households (5.5%) in 2005.[18]

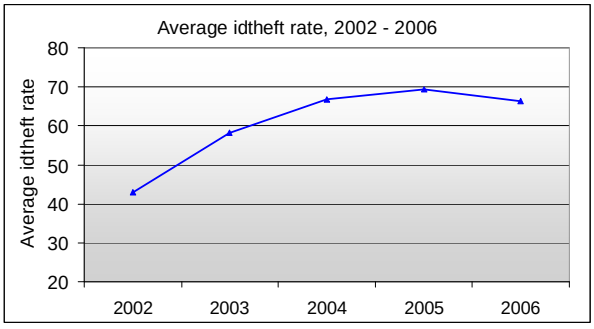
Synovate, on behalf of the FTC conducted national surveys in 2003 and in 2006. The 2003 survey interviewed 4,057 people between March 17th and April 23rd 2003. 4.6% of respondents claimed they were victims of identity theft within the past year, suggesting a total of 10 million victims in 2002. The 2006 survey involved 4,917 interviews conducted between March 27 and June 11, 2006 and found that 3.7% of respondents suffered identity theft, suggesting a total of 8.3 million victims in 2005.[19]

Javelin Strategy and Research conducted surveys in 2003, 2005 and 2006 of around 5000 individuals. Their results show 10.1 million victims (4.7% of the population) in 2002, 9.3 million victims (4.25%) in 2004, and 8.9 million victims (4.00%) in 2005.[20]

In contrast to these surveys, the most comprehensive public source for identity theft data have been the consumer reports published by the FTC since 2002 (further described in Section 5). Summary statistics for annual reported identity thefts are shown in Table 3. A plot of identity theft rates (reports per 100,000 persons) is shown in Figure 2. In 2006, Arizona had the highest reported identity theft rate of 149.2 while Vermont had the lowest, at 28.5.

Table 3: Total Identity Theft reports, 2002-2006

Year	Average	Stdev	Min	Max	Total	% Change
2002	3,040	5,019	81	30,782	155,028	
2003	4,079	6,526	127	39,500	208,033	34.2%
2004	4,705	7,464	179	43,900	239,960	15.3%
2005	4,874	7,621	158	45,180	248,591	3.6%
2006	4,694	7,178	178	41,415	239,391	-3.7%



[18] Note that this survey represents household not individual responses. Since the interviews lasted only 6 months, the 6.4 million figure is an approximate annual estimate. See http://www.ojp.usdoj.gov/bjs/pubalp2.htm#it for more information.

[19] See http://www.ftc.gov/bcp/edu/microsites/idtheft/ for more information.

[20] See http://www.javelinstrategy.com/ for more information.

Figure 2: Identity Theft rate for 2002-2006

These data show identity theft reports increasing at a decreasing rate from 2002 until 2005, after which they decline slightly in 2006.

4.3 Comparison of reported identity theft rates by states with and without law

Prior to 2005, only California had adopted the law, but in 2005, 11 new states adopted the law, [21] and 16 more in 2006. [22] Figure 3 shows the relative changes in reported identity theft rates for three groups: those that adopted in 2005, 2006 and those that, as of the end of 2006, had not adopted the law (23 states[23]).

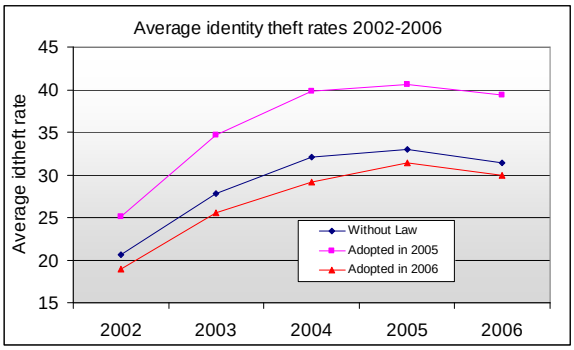


Figure 3: Comparing reported identity theft rates

The figure illustrates how all three trends are increasing at a decreasing rate from 2002 to 2005, after which there is a slight decline in 2006. The average rates of identity theft for states that had not adopted (middle line) reach a maximum of about 33. Identity theft for states that adopted the law in 2006, however, are consistently lower (bottom line, maximum of around 32) while states that adopted in 2005 have higher rates of identity theft (top line, maximum of around 41).

4.4 Data generating Process

The primary effect of data breach disclosure laws is to force firms to notify consumers when their personal information has been lost or stolen. Ideally, as more consumers are notified, more will take precautionary measures to reduce the risk of becoming a victim of identity theft. Conceivably, however, a secondary effect of the law is (given the threat of having to notify consumers) to incentivize firms to improve their security controls *before* they suffer a breach (the sunshine effect). This improvement may reduce the number of data breaches, also reducing the number of identity theft crimes. These cooperative effects are shown below in Figure 4.

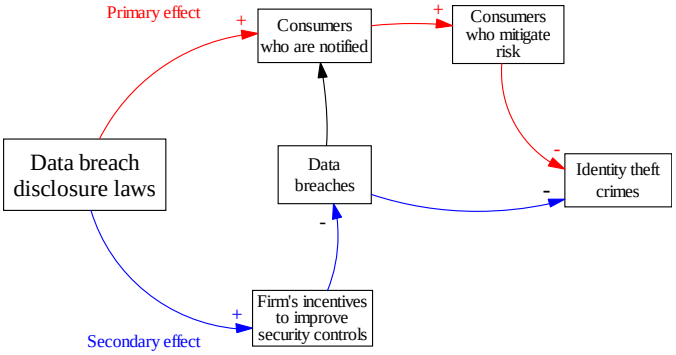


Figure 4: Two effects of data breach disclosure law

[21] Arkansas, Delaware, Florida, Georgia, Nevada, New York, North Carolina, North Dakota, Tennessee, Texas and Washington.

[22] Colorado, Connecticut, Idaho, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nebraska, New Jersey, Ohio, Oklahoma, Pennsylvania, Rhode Island and Wisconsin.

[23] Alabama, Alaska, Arizona, Hawaii, Iowa, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Mississippi, Missouri, New Hampshire, New Mexico, Oregon, South Carolina, South Dakota, Utah, Vermont, Virginia, West Virginia, Wyoming and Washington D.C..

5. DATA ANALYSIS

The Identity Theft Act and Assumption Deterrence Act of 1998[24] criminalized "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. It also empowered the FTC to "log and acknowledge the receipts of complaints by individuals who certify that they have a reasonable belief" that their personally identifiable information has been "assumed, stolen, or otherwise unlawfully acquired." As a result, the FTC established the Identity Theft Data Clearinghouse in November 1999 to collect identity theft complaints from victims. Consumer Sentinel is the web portal by which annual identity theft reports are made available to the public, and where law enforcement can further mine the data.

For our analysis, we use consumer reported identity thefts for each state, including Washington D.C. from the years 2002 to 2006 collected from the FTC. Since only annual data are published, we invoked the Freedom of Information Act to request more granular monthly data. We then aggregated the monthly data into semi-annual time periods (producing 510 observations) since this was the smallest time-frame for which we expected to see an effect of law. This single, federal data source reduces the possibility of inconsistent data collection between states which could lead to erroneous estimations. For example, changes in classification criteria, incentives to report more or less crime, or funding constraints (Blumstein and Wallman, 2006).

Use of self-reported crime data is a familiar issue for criminologists who are often limited by using these data rather than *actual* crimes (e.g. Uniform Crime Reports versus National Crime Victimization Surveys). The frequent under-reporting of crimes is often referred to as the "dark figure" (Biderman and Reiss, 1967) and represents a potential source of error. Blumstein et al. (1991) studied the relationship between reported (UCR) and actual (NCVS) data on burglaries and robberies and found that the UCR and NCVS are "systematically related to each other over time so that value of one series can be estimated with reasonable accuracy from the value of the other." Clearly, their effort benefits from the existence of long-term time series data for both actual and reported crimes but demonstrates that reported crime data can provide reasonable inferences about actual crime trends. To our knowledge, the FTC is the only source for only cross-sectional (state), time series data on identity theft.

5.1 Basic Model

We use state and year fixed effects OLS regression to identify the effect of the breach notification laws on the identity theft rate (identity thefts per 100,000 people). Fixed effects estimation using panel data allows us to control for unobserved heterogeneity at the state level by introducing dummy variables for each state and time period. Identification of the coefficient estimates, therefore, comes from variation across state *and* time. For example, one might expect the numbers of thieves/attackers or a firm's security controls to change over time, which could affect the levels of identity theft. While we do not have measures for these variables, we will assume they are constant across state and will therefore be captured by the time fixed effects. The basic regression model is:

$$\text{idtheft}_{st} = \beta_0 + \beta_1 \text{hasLaw}_{st} + \sum \rho_{st}\, \text{Related}_{st} + \sum \delta_{st}\, \text{Economic}_{st} + \theta_s + \lambda_t + \varepsilon_{st}$$

Where s indexes state and t indexes (6 month) time periods. The dependent variable is identity theft rate (*idtheft*) for state s in period t, and the variable of interest is a dummy variable (*hasLaw*) equal to one when a state adopts the law and zero otherwise. $Related_{st}$ represents credit-related laws that may also affect (prevent) identity thefts. One such legislation is the credit freeze law. These laws enable consumers to apply access control to their credit reports, thereby preventing firms with whom they have no prior agreement to make credit inquiries. If an attacker is trying to open a new account that requires a credit check, they will be stopped and this kind of identity theft will be prevented.[25] The Fair and Accurate Credit Transactions Act (FACTA[26]) is national legislation that was passed as a response to identity theft that allows individuals to request a free annual credit report. This legislation was enacted over the period from 12/01/04 to 09/01/05 beginning with west coast states and ending with east coast states.

$Economic_{st}$ is a vector of state-level economic and demographic controls, as are commonly used in crime analysis (Lott and Mustard, 1997; Donohue, 2004; Donohue and Wolfers, 2006), such as the log of population, state GDP per capita, average state income per capita, and the average unemployment rate over each 6 month period. We also include firm births

[24] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=publ318.105, accessed 02/14/08.

[25] Note that it will not prevent victimization if the attacker uses an existing account.

[26] http://www.ftc.gov/opa/2004/11/facta.shtm, accessed 10/07/07

and deaths per capita. We do not include demographic controls such as race or age composition because we believe these effects remain relatively constant over our five year time window and will therefore be captured by state fixed effects.

Further, as shown in Table 2, there are many causes of identity theft that are not due to data breaches. We believe "Fraud," as recorded by the FTC, is a reasonable proxy for these other sources. Fraud data is collected, managed and reported in a virtually identical method as identity theft and includes such activities as shop-at-home/catalog sales, prizes/sweepstakes, internet auctions, and foreign money offers.

Finally, θ_s and λ_t are state and time fixed-effects and ε_{sy} is the familiar error term. All regressions are run with heteroskedastic robust standard errors clustered-corrected by state. Descriptive statistics are shown in Table 4.

The dates of the adoption of data breach notification laws from January 1, 2002 to December 31, 2006 were obtained from state and federal legislation websites. For the purpose of analysis, we are concerned with the date the law became effective (what we refer to as "adoption"), rather than the date the law was passed. We believe that if the true driver of the law is to create incentives for firms to improve their practices, these incentives will likely only take full force after the adoption of the law. The median delay between passage and adoption is about 4.5 months with a mean of just under 7 months.

State population and GDP data were obtained from the US Census bureau. Unemployment rates were collected from US Department of Labor, Bureau of Labor Statistics. Personal income was gathered from the Bureau of Economic Analysis of the US department of commerce. Firm births and deaths were collected from the US Employment and Training Administration. The FTC provided the fraud data.

5.1.1 Extended Model

It is reasonable to believe that the effect of law may differ across certain demographic characteristics. Our extended model includes the variables listed below.

Demographics: A relevant public policy issue is to consider where these laws would have a stronger effect. For instance, it is reasonable to think that the effect would be stronger in conditions where people are more likely to experience identity theft. The Bureau of Justice, National Crime Victimization Survey on Identity Theft (Baum, 2007) reported greater levels of identity theft for households with higher incomes in more urban locations. To test this, we create two indicator variables, high income and urbanization. We first find the mean of each state's personal income per capita from 2002-2006. High income states are those with average incomes greater than the median ($3,159). We interact high income with the breach law (*Law_HighIncome*). Using data on percent urbanization for each state,[27] we set an indicator variable equal to 1 if the state's percent urbanization is greater than the mean of 68.8%. We then interact urbanization with the state's adoption of the law (*Law_Urban*).

Lagged Law: Next, we consider that the law may not have an immediate effect but that it changes with time. We therefore include an alternative specification replacing *hasLaw* with lagged dummy variables *d1PerOld*, *d2PerOld*, and *d3PerOld*, representing 1 (6 months), 2 (one year) and 3 (1.5 years) or more periods after the law is adopted, respectively.

Strictness of Law: So far, we have assumed that all breach laws are homogenous. We now relax this assumption and consider that some laws may be stricter if they exhibit the following properties: acquisition-based (forcing more disclosure from a lower threshold of breach), cover all entities (businesses, educational and government institutions), higher penalties for fines, no exemptions for GLBA or HIPAA, and encompass more types of personal information (medical, biometric, etc). However, it does not appear that *any* state law satisfies these conditions. Therefore, we relax our requirements and consider a strict law to be one that satisfies two of the original conditions: acquisition-based and covers all persons, businesses and state agencies. Seven states are, therefore, considered to be stricter: California, Florida, Hawaii, Illinois, Nevada, New York, Rhode Island, Tennessee and Washington D.C. We then interact strictness with the state's adoption of the law (*Law_Strict*) to compare states with strict and non-strict laws.

Interstate transactions: Recall from Table 1 that if the majority of personal records are lost or stolen from businesses, we must consider how much of this activity is conducted inter (between) and intra (within) state. If all activity was conducted within the state, for example, then all reported identity thefts would be a result of breaches within that same state. A breach in a university may result in misrecorded reports to the degree that the students are out-of-state residents. However a breach of a state agency (such as a DMV) is likely to only affect residents of that same state. Of the 517 cases analyzed by the CIMIP study (2007), 35% (181) of identity theft crimes occurred out-of-state. Nevertheless, proper identification of the effect of law becomes difficult. We attempt to account for this out-of-state activity in the following three ways:

[27] http://allcountries.org/uscensus/37_urban_and_rural_population_and_by.html, accessed 01/10/08.

- weighting the levels of identity theft by interstate commerce activity as recorded by the 2002 census bureau,
- Conceivably, the adoption of law by neighboring states may affect one's own identity theft rates. Therefore, we include a variable (*percNeighborsLaw*) that represents the percentage of a state's bordering neighbors that have adopted a data breach law.
- To consider the effect on identity theft as more states adopt disclosure laws, we interact the *hasLaw* dummy variable with the percentage of all US states that have adopted the law (*Law_PercStatesWLaw*).

5.2 Results

The results of the regression models are shown in Table 5. The dependent variable in all specifications is the identity theft rate and the variable of interest is *hasLaw*, the effect of data breach disclosure laws.

In specification 1 we regress identity theft on state demographic and economic variables for 2002 to understand how identity theft correlates, if only generally, with a state's demographic and economic indicators. The results suggest that identity theft is highly correlated with the log of population, fraud and state GDP. The interpretation of the population coefficient is that a 10% increase in population increases identity theft by .64 per 100,000 (or 6.4 per 1 million) persons.

Specification 2 and 3 include the same covariates but Specification 3 -- and all other specifications that follow -- use cluster-corrected standard errors by state. We would expect negative coefficients for all of the law-related variables, indicating that their presence reduces the numbers of identity thefts, by either lowering the cost for consumers to check their credit report (FACTA), or providing them with actionable information for which to avoid or prevent becoming a victim. The coefficient of law is -0.05 suggesting that data breach disclosure laws reduce identity thefts by 5 for every 10 million people (a very small amount), however, it is not statistically significant. The coefficient for the effect of credit freeze laws (*hasCreditFreezeLaw*) is positive (1.29) and significant at the 10% level, indicating that credit freeze laws increase identity theft by 1.29 per 100,000 people. However, cluster correcting by state removes all significance.

Specification 4 includes interactions of a state's law with higher income, more urban areas and strictness of law. The interpretation of the coefficient of *Law_HighIncome*, for example, suggests that having a data breach disclosure law in a richer state reduces identity thefts by about 1.9 in 100,000 and is significant at the 10% level. Neither *Law_Urban* nor *Law_Strict* have either economically or statistically significant coefficients. Together, these findings suggest that the laws in more urban states or stricter laws do not reduce identity theft more than weaker ones (as defined by the authors).

Specification 5 shows the effect of the lagged adoption of law. The results indicate that 6 months after adoption, identity thefts increase by about 1.2 per 100,000 and is significant at the 5% level. Periods of 12 and 18 months after adoption, however, are statistically insignificant, indicating the lack of stronger effect over time.

The dependent variable in Specification 6 weights the identity theft rate by the percentage of interstate commerce as an attempt to compensate for consumer reports in one state that could have actually occurred in another state. The coefficient of law is negative but small (-0.19) and again insignificant.

Finally, Specification 7 accounts for interstate transactions by considering the percent of neighboring states with the law and an interaction of law with percentage of total states with the law. The coefficient representing the percent of neighboring states with the law (*percNeighborsLaw*) is small, but positive (3.16) and significant at the 5% level. The interpretation is that, as 10 more percent of one's neighbors adopt the law, identity theft reporting rates increase by 32 in 100,000. The interaction of law with the percentage of all US states with the law shows a positive but non significant effect (0.78).

Alternative specifications were also run using the log of identity theft rates as the dependent variable. While this produced slightly smaller standard errors, it does not substantially affect the results.

5.2.1 Reporting bias

We cannot avoid the possibility of reporting bias -- that those who report identity thefts are systematically different from those who experience the crime. Biases could be due to the amount of stolen money or type of identity theft suffered by the victim. For instance, Blumstein et al. (1991) found that, "offences involving injury to the victim or substantial property loss are more likely to be reported to the police" (and similarly suggesting that less severe offences could be underreported). In 2005, the Bureau of Justice found that about 45% of victims experienced identity theft relating to existing credit card accounts (generally considered a less severe form of identity theft) (Baum, 2007) whereas the FTC consumer complaints from 2004 to 2006 ranged between 10.7% and 11.9% for the same type of identity theft (FTC, 2007). The relatively low reporting rate relative to survey data (about ¼ as much), suggests an underreporting of less severe forms of identity theft.

Another potential source of error could be due to underreporting of crimes where offenders are known to the victims (Garofalo, 1990). Javelin (2006) reports that about 15% of known causes of identity theft were by someone the victim knew

(friend, acquaintance, or relative), whereas FTC-Synovate (2007) reports a similar 16%. While the FTC complaint form does allow the respondent to specify their relationship to the offender, this information is not published in the annual consumer reports and was unavailable at the time of writing.

From 2004 to 2006, the FTC (FTC, 2007) identifies the 18-29 year old cohort consistently reporting more identity thefts and that those aged 60 and over report the least frequently. Similar proportions are supported by the FTC-Synovate (2007) and BJS victim surveys (Baum, 2006, 2007) and therefore suggests little age bias reporting. The FTC complaint forms[28] do not collect victim demographic information such as income, education, race, or ethnicity, so we are therefore unable to estimate the degree to which these factors may cause a reporting bias.

While not conclusive, these findings suggest that any biases that may exist are more a function of the type of crime, rather than specific characteristic of the victim.

6. POLICY IMPLICATIONS

A broader issue relevant to policy makers is whether there are other means by which this law could (and should) be evaluated. Environmental disclosure laws often measure a deterrent policy by their effectiveness at reducing not just the frequency of incidents, but also the severity of incidents and a firm's compliance with the regulation (Cohen, 2000). While our analysis may not show conclusively that the laws reduce the frequency of identity thefts, it is possible that they could help reduce the severity of the crimes (as measured by consumer losses or type of identity theft), or compliance, as measured by the improvement in a firm's security practices.

6.1 Consumer losses and incentives

Studies have shown that a victim loses less money the sooner they become aware of fraudulent activity (FTC-Synovate, 2007; Javelin Research, 2006). Javelin claims that losses are 21% lower when consumers detect identity theft within the first week, and 65% lower when consumers detect the crime within a year. Moreover, they claim that average consumer costs declined in 2005 by 37% ($422). However, once notified, the responsibility still lies with the individual to take mitigating actions, something which not everyone appears do be doing. Robert Kamerschen, vice president of Choicepoint, claimed that fewer than 10% of the 163,000 consumers availed themselves of free credit monitoring services following the Choicepoint breach.[29] Moreover, FTC-Synovate (2006) found that 44% of identity theft victims ignored breach notification letters. A recent Ponemon survey discovered that 77% of respondents claimed to be concerned or very concerned about loss or theft of personal information and 72% of respondents believed that their chances of becoming a victim of identity theft was greater than 20%. Yet, despite these claims of concern, 65% of respondents failed to take advantage of free or subsidized credit monitoring services.

It is possible that these behaviors are manifestations of a number of human behavior decision errors (Loewenstein, John, Volpp, in preparation):

- optimism bias: consumers simply perceive their chances of becoming a victim to be very low
- rational ignorance: consumers believe their cost of obtaining more information about how to respond outweighs any benefits that they may receive
- status quo bias: consumers' own inertia inhibits them from anticipating possible future consequences of identity theft and responding appropriately.

Just as Magat and Viscusi (1992) argue, disclosure legislation will be more effective when the notices contain the necessary information required for consumers to better evaluate the risk and take appropriate measures to prevent loss. For example, there is evidence that very few disclosure letters contain full information and inform consumers of the data that was actually compromised (which becomes relevant when you consider the consequences of loss of SSN vs one's home address and phone number) (Samuelson Law, 2007). Moreover, the letters often lack customer support contact information, and we have yet to hear of a letter that emphasizes the average costs to consumers from breaches or cite the millions of estimated victims of identity theft each year. Therefore, including relevant information may help overcome both optimism bias and rational ignorance.

Finally, we recognize that many breaches result in no consumer loss, either because the information was simply lost and will never be used maliciously, or when one's merchant bank reimburses the consumer of credit card fraud. However, until the

[28] The FTC identity theft complaint form: https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03, accessed 02/20/08.

[29] http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html, accessed 02/13/08.

crime occurs, one does not know a priori whether they will suffer loss and so rather than relying on the consumer to take action (for example, by signing up for identity theft insurance, fraud alert, or credit freeze), we consider that any one of these mitigating actions could be implemented without delay, on behalf of the customer, thereby alleviating the status quo bias.

6.2 Firm losses and incentives

But firms may likely suffer from optimism bias, too. They may believe their probability of suffering a breach is small enough that, despite a few very highly publicized breaches, may still not fully appreciate (or internalize) the penalties. For example, Choicepoint incurred a total of $26M in fines and fees. They were fined $10M by the FTC for violating the fair credit reporting act, and required to allocate a $5M trust fund to assist identity theft victims (redress). They suffered a $10M civil class-action lawsuit, paid an additional $500k for many states' legal fees, and spent $500k toward an identity theft education campaign.[30] And they survived. Moreover, their assets (consumer personal information) are valuable enough that they became a recent acquisition target by Reed Elsevier, the parent company of LexisNexus.[31] In addition, TJ Max reported costs of $178M for a breach that was disclosed in early 2007 and involved 95 million customer records. Despite this, their profits increased by $1.66 per share one year later.[32]

A number of studies have examined the financial impacts to firms that incurred a privacy or security breach, with most showing only a mild effect. Campbell et al. (2003), for instance, find "limited evidence of an overall negative stock market reaction to public announcements of information security breaches." Cavusoglu et al. (2004) find that the disclosure of a security breach results in the loss of $2.1 of a firm's market valuation. Acquisti, Telang and Friedman (2006) use an event study to investigate the impact on stock market prices for firms that incurred a privacy breach. They found a negative and significant, but temporary reduction of 0.6% of the stock market price on the day of the breach. Ko and Dorantes (2006) study the four financial quarters post security breach. They find that while the firm's overall performance was lower (relative to firms that incurred no breach), the breached firm's sales increased significantly relative to firms that incurred no breach. Regardless of these findings, firms do appear to be making significant security and operational improvements in the wake of disclosure laws (Samuelson, 2007).

6.3 Recommendations

Proper research on the effectiveness of data breach disclosure laws is hampered by the lack of sufficient, high quality data. Hoofnagle argues that the current collection of identity theft records come from surveys and anecdotal accounts (Hoofnagle, 2007). He claims that current information is not sufficient and that banks and other organizations should be required to release identity theft data to the public for proper research. We certainly agree with this view. To the extent that reporting and other biases can be reduced, it will allow researchers to more accurately measure the impact of disclosure laws. Moreover, we believe that the proper collection of identity theft victimization, and consumer and firm loss data will be a valuable tool for researchers, policy makers and consumers. We therefore join others (Samuelson, 2007) in supporting the following recommendations to policy makers:

- Create a single, federal data breach disclosure law that covers all persons, private organizations, data brokers and state and federal agencies. This single law should reduce conflict between states laws and lower the barrier for compliance.
- Standardize the content of notifications to include only pertinent information (no marketing brochures) that includes actionable information for the consumer (e.g. date of breach, type of personal information lost, and customer support contact information).
- Define an oversight committee to be notified of all breaches. This will create an authoritative source of breach data that can be made available to policy makers, researchers and consumers.

7. CONCLUSION

We have researched the effect of data breach disclosure laws on identity theft, though we find no statistically significant result. However, this lack of significant findings may be due to a number of factors:

There could be a significant and negative effect, but our regression model is too blunt an instrument with which to properly identify it. The fixed-effects regression with panel data is a powerful econometric method that allows us to control

[30] http://www.networkworld.com/news/2008/012908-choicepoint-to-pay-10m-to.html, accessed 02/13/08.

[31] http://www.washingtonpost.com/wp-dyn/content/article/2008/02/21/AR2008022100809_pf.html, accessed 02/23/08.

[32] http://www.networkworld.com/nlsecuritynewsal88931, http://www.theregister.co.uk/2007/12/20/tjx_bank_settlement/, accessed, http://money.cnn.com/2008/02/20/news/companies/bc.earns.tjx.ap/index.htm accessed 02/20/08.

for unobserved heterogeneity in addition to numerous demographic and economic factors. We consider that the overall effectiveness of law may vary by state income, urbanization and strictness of law and we accounted for credit-related legislations that may lead to increased reporting. We test the possibility that an identity theft that occurs in one state may be misreported in another state and whether the effect of law varies with time. Nevertheless, we recognize the possibility of confounding factors that may lead to omitted variable bias. This may occur when some states exhibit a systematically higher proportion of identity theft reporting than other states. Note that national trends would be captured by the time fixed-effects in the regression model. Moreover, our results would represent a lower bound on the overall effect of law.

While reported crime data is commonly used as a proxy for actual crimes, we cannot rule out the possibility that data from the FTC may still somehow be biased. This would therefore, restrict our inferences about the true effect of law on all identity theft crime. Nevertheless, we can rule out some sources of bias, and we believe the data collected and published by the FTC is currently the best source of identity theft data.

The laws could simply not be effective at reducing the number of identity theft victims. If the vast majority of identity theft does not originate from data breaches, then the maximum effectiveness of these laws is inherently limited. It is also possible that firms have simply not had the time to properly implement the necessary security controls, or that the controls they have implemented are not effective at preventing breaches. Conditional on being notified, however, the consumers must themselves take responsibility to reduce their own risk of identity theft – something which only a minority appear to be doing. And so it may be that only with time, will we see more firms internalize the costs, more consumers respond to the risks, and the victimization rates decline.

8. ACKNOWLEDGMENTS

The authors would like to Katrina Baum, Al Blumstein, John Hutchins, Jed Kolko, Andrew Moore and Peter Swire, for their valuable suggestions. Special thanks to Anand Nandkumar for his continued feedback and insights.

9. APPENDIX

9.1 Tables

Table 4: Descriptive Statistics

Variable	Mean	Std. Dev	Min	Max
Identity theft rate	30.39	14.29	5.67	84.86
Has data breach law	0.14	0.34	0	1
Has FACTA	0.40	0.49	0	1
Has Credit Freeze Law	0.09	0.28	0	1
d1PerOld (6 month old law)	0.05	0.21	0	1
d2PerOld (12 month old law)	0.02	0.15	0	1
d3PerOld (18 month old law)	0.01	0.12	0	1
% Neighbors with law	0.13	0.23	0	1
State GDP per capita	3,666.95	1,299.12	2,257.97	12,623.37
Income per capita	3,255.50	564.27	2,128.98	5,803.40
Unemployment rate	5.10	1.12	2.18	8.55
ln(population)	15.06	1.04	13.12	17.41
Firm birth rate	322.10	111.18	173.62	757.78
Firm death rate	337.11	103.68	165.95	759.66
Fraud rate	57.23	19.36	16.79	180.28

Table 5 : Regression Results

Dependent variable (1-4,7): identity theft rate Dependent variable (6): identity theft rate weighted by interstate commerce							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
COEFFICIENT	2002 Only	Basic	SE cluster-corrected	Extended	LaggedLaw	Weighted	Neighbors
hasLaw		-0.03	-0.03	0.72		-0.19	-0.26
		(0.60)	(0.63)	(0.73)		(0.37)	(1.13)
hasfacta		-0.05	-0.05	-0.03	-0.00	0.52	-0.07
		(0.65)	(0.59)	(0.59)	(0.60)	(0.38)	(0.57)
hasCreditFreezeLaw		1.29*	1.29	1.52	1.29	1.05	1.13
		(0.72)	(1.15)	(1.22)	(1.08)	(0.88)	(1.15)
Law_HighIncome				-1.85*			
				(0.94)			
Law_Urban				0.35			
				(0.96)			
Law_Strict				-0.08			
				(1.06)			
d1PerOld					1.23**		
					(0.58)		
d2PerOld					-1.79		
					(1.39)		
d3PerOld					0.24		
					(1.24)		

%NeighborsWLaw							3.16**
							(1.38)
Law*%StatesWLaw							0.78
							(2.88)
stategdpper	0.00***	-0.00*	-0.00*	-0.00**	-0.00*	-0.00*	-0.00*
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
incomeper	-0.00*	-0.00	-0.00	-0.00	-0.00	-0.00	-0.00
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
unemp	0.56	0.04	0.04	0.02	0.09	-0.37	-0.01
	(0.74)	(0.36)	(0.52)	(0.52)	(0.52)	(0.27)	(0.54)
lnpop	6.45***	88.64***	88.64***	91.58***	94.60***	48.49***	89.45***
	(0.84)	(12.74)	(26.31)	(26.31)	(26.67)	(17.10)	(26.51)
firm_birthsper	0.01	-0.01	-0.01	-0.01	-0.01	-0.01**	-0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
firm_deathsper	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	(0.01)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
fraudper	0.44***	-0.01	-0.01	-0.01	-0.01	-0.01	0.00
	(0.08)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)
dper2		5.23***	5.23***	5.22***	5.19***	2.13***	5.16***
		(0.61)	(0.42)	(0.42)	(0.41)	(0.28)	(0.41)
dper3		11.00***	11.00***	10.97***	10.91***	4.29***	10.86***
		(0.69)	(0.71)	(0.70)	(0.69)	(0.46)	(0.69)
dper4		9.17***	9.17***	9.11***	9.06***	3.58***	8.94***
		(0.77)	(0.65)	(0.63)	(0.62)	(0.50)	(0.61)
dper5		16.27***	16.27***	16.17***	16.13***	6.45***	15.95***
		(0.87)	(1.04)	(1.01)	(1.00)	(0.77)	(0.96)
dper6		12.95***	12.95***	12.77***	12.84***	4.91***	12.57***
		(1.01)	(0.96)	(0.93)	(0.95)	(0.76)	(0.86)
dper7		18.53***	18.53***	18.25***	18.36***	6.83***	17.93***
		(1.10)	(1.13)	(1.09)	(1.11)	(0.97)	(0.99)
dper8		13.40***	13.40***	13.12***	13.11***	4.69***	12.24***
		(1.40)	(1.36)	(1.34)	(1.36)	(1.08)	(1.29)
dper9		18.20***	18.20***	17.82***	17.89***	6.21***	16.40***
		(1.53)	(1.58)	(1.58)	(1.56)	(1.24)	(1.54)
dper10		10.59***	10.59***	10.10***	10.35***	2.89**	8.39***
		(1.56)	(1.59)	(1.67)	(1.58)	(1.26)	(1.61)
d1PerOld					1.23**		
					(0.58)		
d2PerOld					-1.79		
					(1.39)		
d3PerOld					0.24		
					(1.24)		
Constant	-103.53***	-1,289.65***	-1,289.65***	-1,334.66***	-1,379.62***	-705.11***	-1,303.20***

	(10.95)	(192.40)	(395.17)	(394.93)	(400.64)	(258.38)	(398.19)
Observations	102	510	510	510	510	510	510
Number of stateid		51	51	51	51	51	51
R-squared	0.77	0.81	0.81	0.81	0.81	0.68	0.81

Standard errors in parentheses, *** p<0.01, ** p<0.05, * p<0.1

10. REFERENCES

Akers, R. L. and Sellers, C. S., "Criminological Theories: Introduction, Evaluation, and Application," Roxbury Publishing Company, 2004.

Acquisti, A., Friedman, A. and Telang, R., Is There a Cost to Privacy Breaches? An Event Study, Fifth Workshop on the Economics of Information Security, 2006.

Arora, A., Telang, R. and Xu, H., "Optimal Policy for Software Vulnerability Disclosure," The Third Annual Workshop on Economics and Information Security (WEIS04), 2004.

Black, D. A. and Nagin, D. S., "Do Right-to-Carry Laws Deter Violent Crime?" National Consortium on Violence Research, Carnegie Mellon University, 1996.

Biderman, A. D. and Reiss, Jr., A. J., "On Exploring the "Dark Figure" of Crime," Annals of the American Academy of Political and Social Science, Vol. 374, Combating Crime, Nov., 1967,

Blumstein, A., Cohen, J. and Nagin, D., "Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates, Report of the Panel of Deterrence and Incapacitation," National Academy of Sciences, Washington, D.C., 1978.

Blumstein, A. and Wallman, J., "The Crime Drop and Beyond," Annual Review of Law & Social Science, Vol. 2, December 2006.

Blumstein, A, Cohen, J. and Rosenfeld, R., "Trend and Deviation in Crime Rates: A Comparison of UCR and NCS Data for Burglary and Robbery," Criminology 29 (2): 237-263, 1991.

Baum, K., "Identity Theft, 2004," Bureau of Justice Statistics Special Report, NCJ 212213, April 2006.

Baum, K., "Identity Theft, 2005," Bureau of Justice Statistics Special Report NCJ 219411, November 2007.

Campbell, K., Gordon, L. A., Loeb, M. P. and Zhou, L., "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, 11, 431-448, 2003.

Cavusoglu, H., Mishra, B.and Raghunathan, S., "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," International Journal of Electronic Commerce , Volume 9, Issue 1, 2004.

Cohen, M. A., "Optimal Enforcement Strategy to Prevent Oil Spills: An Application of a Principal-Agent Model with Moral Hazard," Journal of Law and Economics, Vol. 30, No. 1, pp. 23-51, 1987.

Cohen, M. A. "Empirical Research on the Deterrent Effect of Environmental Monitoring and Enforcement," Environmental Law Reporter, 30: 10245-52 (April 2000).

Cloninger, D. O., "The Deterrence Effect of Law Enforcement: An Evaluation of Recent Findings and Some New Evidence," American Journal of Economics and Sociology, Vol. 34, No. 3, July, 1975.

Donohue, J. and Ayres, I., "Shooting Down the 'More Guns, Less Crime' Hypothesis," Stanford Law Review 51.4, 2003.

Donohue, J., "Guns, Crime, and the Impact of State Right-to-Carry Laws" Fordham Law Review 73, 2004.

Epple, D. and Visscher, M., "Environmental Pollution: Modeling Occurrence, Detection and Deterrence," Journal of Law and Economics, 1984.

Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data: January-December 2006," Federal Trade Commission, February 2007.

Federal Trade Commission, "FTC Identity Theft Survey Report: 2003," Federal Trade Commission, 2003.

Federal Trade Commission, "FTC Identity Theft Survey Report: 2007," Federal Trade Commission, 2007.

Garofalo, J., “The National Crime Survey, 1973-1986: Strengths and Limitations of a Very Large Data Set," In MacKenzie, Doris L., Phyllis Jo Baunach, and Roy R. Roberg (eds), “Measuring Crime: Large-Scale, Long-Range Efforts,” Albany: State University of New York Press, 1990.

Gordon, G. R. et al. “Identity Fraud Trends and Patterns: Building a data-based foundation for proactive enforcement” Center for Identity Management and Information Protection, Utica College, 2007.

Givens, B. “Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions,” Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, July 12, 2000.

Helland, E., "The Enforcement Of Pollution Control Laws: Inspections, Violations, And Self-Reporting," The Review of Economics and Statistics, MIT Press, vol. 80(1), pages 141-153, 1998.

Hamilton, J. T., “Pollution as News: Media and Stock Market Reactions to the Toxics Release Inventory Data,” Journal of Environmental Economics and Management, Volume 28, Issue 1, Pages 98-113, 1995.

Hoofnagle, C. J. "Identity Theft: Making the Known Unknowns Known," Harvard Journal of Law and Technology, Vol. 21, 2007.

Hutchins, J. P. (ed), Data breach disclosure laws - State by State," American Bar Association, 2007.

Javelin Research, "Identity Fraud Survey Report: 2006," Javelin Strategy & Research, 2006.

Javelin Research, "Identity Fraud Survey Report: 2007," Javelin Strategy & Research, 2007.

Jin, G. Z. and Leslie, P., "The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards" The Quarterly Journal of Economics, pages 409-451, May, 2003.

Jovanovic, B. "Truthful Disclosure of Information," Bell Journal of Economics, The RAND Corporation, vol. 13(1), pages 36-44, 1982.

Ko, M, and Dorantes, C., "The impact of information security breaches on financial performance of the breached firms: an empirical investigation," Journal of Information Technology Management, Volume XVII, Number 2, 2006.

Konar, S. and Cohen, M. A.,"Information As Regulation: The Effect of Community Right to Know Laws on Toxic Emissions," Journal of Environmental Economics and Management, Elsevier, vol. 32(1), pages 109-124, 1997.

Lenard, T. M. and Rubin, P. H. "Slow Down on Data Security Legislation." Progress Snapshot 1.9. The Progress & Freedom Foundation, August 2005.

Lenard, T. M. and Rubin, P. H., "Much Ado about Notification". Regulation, Vol. 29, No. 1, pp. 44-50, Spring 2006.

Levitt, S. D., "Why Do Increased Arrest Rates Appear to Reduce Crime: Deterrence, Incapacitation, or Measurement Error?" NBER Working Paper No. W5268, September 1995.

Loewenstein, G., John, L, & Volpp, K. (in preparation), “Using decision errors to help people help themselves” In E. Shafir (Ed.), The Behavioral Foundations of Policy. Princeton, NY: Princeton University Press.

Lott, Jr., J. R. and Mustard, D. B., "Crime, Deterrence and the Right-to-Carry Concealed Handguns,” University of Chicago: Journal of Legal Studies, January 1997.

Magat, W. A. and Viscusi, W. K. "Informational approaches to regulation," MIT Press, 1992.

Mathios, A. "The Impact of Mandatory Disclosure Laws on Product Choices: An Analysis of the Salad Dressing Market," Journal of Law and Economics, Vol. 43, No. 2, October 2000.

Mocan, H. N., and Gittings, K, “Getting Off Death Row: Commuted Sentences and the Deterrent Effect of Capital Punishment,” Journal of Law and Economics, October 2003.

Nagin, D., "General Deterrence: A Review of the Empirical Evidence," in Alfred Blumstein, Jacqueline Cohen, and Daniel Nagin (eds.), Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime (Washington, D.C.: National Academy of Science, 1978).

Nagin, D., "Criminal Deterrence research at the outset of the twenty-first century," Crime and Justice, Volume 23, 1998.

Polinsky, A. M and Shavell, S. "Mandatory versus Voluntary Disclosure of Product Risks" (October 2006). Stanford Law and Economics Olin Working Paper No. 327.

Ponemon Institute, "National Survey on Data Security Breach Notification", The Ponemon institute, 2005.

Ponemon Institute, "The Business Impact of Data Breach," The Ponemon Institute, 2007.

Ranger, S. “Data breach laws 'make companies serious about security,” Silicon.com, 2007, http://management.silicon.com/itdirector/0,39024673,39168303,00.htm?r=1, Accessed Oct 27, 2007.

Robinson, P. H. and Darley, J. M., "The Role of Deterrence in the Formulation of Criminal Law Rules: At Its Worst When Doing Its Best" . Georgetown Law Journal 949-1002, 2003.

Samuelson Law, Technology, & Public Policy Clinic, “Security Breach Notification Laws: Views from Chief Security Officers,” University of California-Berkeley School of Law, December, 2007.

Science and Technology Committee, "Personal Internet Security," House of Lords, Science and Technology Committee, 5th Report of Session 2006–07, HL Paper 165–I, 2007.

Schwartz, P and Janger, E. "Notification of Data Security Breaches," 105 Michigan Law Review 913, 2007.

Shavell, S. "A Note on the Incentive to Reveal Information," Discussion Paper, No. 25, Program in Law and Economics, Harvard Law School, 1987.

Swindle, O. G. and Ross, P. "Managing Information and its Security: The Role of Policymakers, the Private Sector and Consumers," Progress & Freedom Foundation Progress on Point Paper No. 13.2, 2006.

US Congress, “Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs,” 109th Congress, 2005.

US Congress, “Assessing Data Security: Preventing Breaches and Protecting Sensitive Information: Hearing Before the House Comm. on Financial Services,” 109th Congress, 2005.

US Congress, “Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary,” 109th Congress, 2005.

US Congress, “Securing Consumers’ Data: Options Following Security Breaches: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce,” 109th Congress, 2005.

Van Dyke, J. "Reading behind the lines: How Identity Fraud Really Happens," Javelin Strategy & Research, 2007.

Wolfers, J. and Donohue, J. J., "Uses and Abuses of Empirical Evidence in the Death Penalty Debate" CEPR Discussion Paper No. 5493, February 2006.

Wood, D. "GAO-07-737 Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," Government Accountability Office, 2007.