# 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**

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 identity theft, 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 2007. We find that adoption of data breach disclosure laws have marginal effect on the incidences of identity thefts and reduce the rate by just under 2%, on average. While this effect is marginal, reducing identity theft is only one means by which these laws can be evaluated: we appreciate that they may have other benefits such as reducing the average victim's losses or improving a firm's security and operational practices.

**Keywords**

Data breach disclosure, security breach, economics of information security, identity theft, fixed-effects regression

## 1. INTRODUCTION

Consumer identity theft resulted in corporate and consumer losses of around $56 billion dollars[1] 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. However, to date, no empirical analysis has investigated the effectiveness of such legislative initiatives in reducing identity theft. In this paper, we use panel data gathered from the Federal Trade Commission (FTC) over a five year time period to empirically examine this effect.

### 1.1 Motivation for data breach disclosure laws

The spirit of the data breach notification laws are contained within two phrases: "*Sunlight as a disinfectant*,"[2] 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).

[1] 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 stolen/victim = $56.6B. (Actual amount lost per consumer was $422 on average.)

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

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.

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, their credit card merchant, the FTC, or law enforcement; they can close unused financial accounts; they can place a credit freeze or fraud alert on their credit report.[3] 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. It has been shown that consumers lose confidence in firms who suffer breaches (Ponemon, 2005). However, it may only be through legislation that firms acquire sufficient incentive to actually improve their practices to reduce the likelihood of future breaches and repair consumer confidence.

At least four US congressional hearings have convened to discuss how data breach laws may reduce identity theft (US Congress, 2005a, 2005b, 2005c, 2005d), and a special report from the US Government Accountability Office (GAO) discussed the connection between data breach disclosure laws and identity theft (Wood, 2007). Further, many state laws specifically address identity theft prevention.[4]

Finally, 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 creates unnecessary costs for firms and consumers. They argue, for example, that if the probability of a consumer suffering identity theft is low, then both firms and consumers could incur unnecessary costs by overreacting (Lenard and Rubin, 2005, 2006). 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, these policies may impede e-commerce and stifle technological development by discouraging firms to innovate using consumers' personal information (or stop collecting it altogether)[5]. Lenard and Rubin also consider how firms are burdened by complying with multiple, disparate, and perhaps conflicting disclosure laws. They further note that these laws are unnecessary because of the following:

- The probability of becoming a victim of identity theft as a result of a data breach is very low, around only 2%.

---

[3] 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.

[4] Californian legislators consider their data breach law as a possible remedy for identity theft: "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." (SB1386). Other state laws specifically address identity theft prevention (e.g Hawaii, SB2290; Michigan, SB309; Montana, SB732; South Carolina, SB1048; NH, HB1660; NJ, A4001; OR, SB583; RI, HB6191). For example, the Hawaii law states, "The purpose of this Act is to alleviate the growing plague of identity theft by requiring businesses and government agencies that maintain records containing resident individuals' personal information to notify an individual whenever the individual's personal information has been compromised by unauthorized disclosure." Montana's breach law is "an act adopting and revising laws to implement individual privacy and to prevent identity theft."

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

- The externality is not as severe as claimed because around 90% of the cost of identity theft and fraud is already born by the firms (businesses, banks, credit card issuers, merchants). [6]
- 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.

Many strongly oppose the idea of government regulations. For example, a recent article in the Wall Street Journal argues that because of the speed by which online attacks change, more legislation would simply produce a lowest threshold of compliance, "[o]ur 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 a few years from now."[7] 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."

In summary, these arguments present a stimulating debate as to whether data breach disclosure laws can and should 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 2007, we use state and year fixed effect regression analysis to empirically estimate the impact of data breach laws on the frequency of identity thefts.

After incorporating various controls, we find that adoption of data breach disclosure laws reduce the identity theft rate by just under 2%, on average. While this effect is marginal, it appears to be within the norm of other forms of information disclosure policies. The lack of a strong 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 sampling bias also potentially affect our identification.

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 present results in Section 6. Discussion, policy implications and conclusions are presented in Sections 7, 8 and 9, respectively.

## 2. RELATED WORK

Our paper draws from multiple literatures. First, we draw from the literature on policy making and firm disclosures: when do firms have incentives to disclose favorable (as well as unfavorable) information? We also draw from literature in crime policy and information security economics.

### 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. Legislations forcing firms to disclose information and their effectiveness have been widely studied. Shavell (1987) examine producers' incentives to reveal favorable information and conceal unfavorable information. He shows that sellers with low quality goods conceal information about their products and free ride off of competitors with better quality goods. 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 it 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)."

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

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

Researchers have also studied health information disclosure in the restaurant industry (Jin and Leslie, 2003). Specifically, Jin and Leslie find that disclosing the hygiene quality of a restaurant increases health inspection scores and lowers the occurrence of food borne diseases. Moreover, and importantly, this is a credible signal to consumers who respond by demanding cleaner restaurants.

Mathios (2000) examines the effects 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. Mathios further describes other models that predict how voluntary disclosure leads to "partial unraveling of information." For instance, firms don't voluntarily disclose when it's costly, or when they can't credibly "convey the information."

A number of studies have examined the financial impacts to firms that disclose a privacy or security breach. Most show only a mild effect. Campbell, Gordon, Loeb and Zhou (2003), for instance, find “limited evidence of an overall negative stock market reaction to public announcements of information security breaches.” However, they do find a significant and negative effect on stock price specifically for breaches caused by “unauthorized access of confidential information.” 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. Telang and Wattal (2007) find that software vendors’ stock price suffers when vulnerability information in their product is announced. Acquisti, Telang and Friedman (2006) use an event study to investigate the impact on stock market prices for firms that incurred a privacy breach and 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).

Disclosure is also studied in the context of releasing software vulnerability information to the public. This has been a contentious topic and many users try to disseminate vulnerability information without giving the vendors a chance to release the patch. Arora, Telang and Xu (2008) discuss the role of a policy maker in setting an optimal time to disclose software vulnerabilities. They find that software vendors wait longer than is socially optimal to release a patch and threat of disclosure can force the vendors the release the patch early. See Li and Rao (2007) for a detailed discussion on vulnerability disclosure policies.

## 2.2 Environmental Disclosure and Deterrent Policies

There is a strong precedent of disclosure legislation in the United States. The Food and Drug Administration (FDA) and the Environmental Protection Agency (EPA) have various regulations which require that a firm notify consumers in case of an adverse impact of their products and services. A specific example of EPA efforts is the Toxic Release Inventory (TRI) program developed by the Environmental Protection Community Right to Know Act (EPCRA). 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) studied alternative environmental deterrence policies on environmental disasters. Specifically, he examined 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.

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). For example, a meta-analysis by Donohue (2004, Figures 1-9) of the effect of concealed handgun laws (right-to-carry) on violent crime reveals a range of estimates from about -3% to 4% (statistically significant aggregate estimates). Similarly, they present a range of zero to almost 10% of the effect of the laws on property crime. While there appears to be no conclusive evidence to overwhelmingly support deterrence policies, for the purpose of this study, we gained valuable methodological insight from the 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."[8] 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 in Table 1.[9] The data represent 773 breaches of US organizations collected by Attrition.org from the years 2002 to 2007.

[Insert Table 1 : Summary Statstics of soures of data breaches]

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. They may detect the breach themselves. 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.

---

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

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

## 3.2 US Data Breach Disclosure Legislation

As we noted earlier, due to increasing number of data breaches and identity thefts, many states are adopting data breach disclosure laws. As of December 31, 2007, 38 US states had adopted data breach legislation, as shown in Figure 1 and Table 2[10] in the Appendix.

[Insert Figure 1: Adoption of breach notification laws from 2002 to 2007]

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 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 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). Other states adopt similar definitions.

*Personally Identifiable Information (PII)*: Generally, PII includes part of a consumer's name in addition to another piece of identifiable information. There are minor differences across the states, however. 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. Seventeen states require notification when the personal information is reasonably assumed to have been acquired by an unauthorized party. Whereas other states require notification only if it is reasonable to believe the information will cause harm to consumers.

*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. The specificity of Georgia's law is likely due to the fact that Choicepoint, the data broker that suffered the very popular data breach in 2005, is headquartered in Georgia.

*Notification*: Notification refers to the timeliness by which the firm must notify the consumer. It also describes to whom notifications must be sent - 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, Indiana, Michigan and Minnesota provide exemption for financial firms if they are governed by the Gramm-Leach-Bliley Act (GLBA). Arizona, Hawaii and Indiana provide exemption for firms governed by the Health Insurance Portability and Accountability Act (HIPAA). Other exemptions are provided: if the firm has contacted law enforcement and they believe consumer notification may jeopardize an 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 retribution by the state attorney general or a civil right of action. Many states do not specify a maximum civil penalty. However, the Arizona and Arkansas laws allow a civil penalty not exceeding $10,000, whereas the limit is $25,000 in Connecticut and Idaho, and $500,000 in Florida.

[10] 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.

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 which also serves Californian consumers incurs a breach, it must notify any consumer that resides in California. Of course, not all breaches affect consumers in every state. Breaches in state government agencies, community colleges, schools and hospitals likely only affect residents of a single state. Even breaches by national firms may only result in the compromise of a group of individuals (often employees) of a single state.

### 3.3 Conceptual Model

We now outline our conceptual model and how the laws are expected to impact identity theft crimes. Figure 2 outlines our model and 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. For example, they could call their financial institutions.

[Insert Figure 2: Two effects of data breach disclosure law]

Conceivably, however, given the costs of having to notify consumers (from tangible costs to intangible costs such as negative reputation effects), a secondary effect of the law is to incentivize firms to improve their security controls before they suffer a breach (the *sunshine* effect). Breaches are usually associated with bad publicity and affect the firm's reputation, sometimes causing financial losses (Acquisti, Friedman, Telang 2007). This improvement may reduce the number of data breaches, also reducing the number of identity theft crimes. Both effects (consumers taking precautions and firm investing in better security) should reduce the incidences of identity thefts.

It is tempting to investigate the effect of disclosure laws on data breaches (rather than identity theft). However, a significant data problem emerges. While the numbers of state-level breaches over time are known, these largely reflect only reported breaches post-law. Actual numbers of breaches, especially during the pre-law period, are likely greater than observed, but of course firms chose not to disclose because it was not required.

## 4. IDENTITY THEFT DATA

### 4.1 Data Sources and Summary Statistics

The most comprehensive public source for identity theft data have been the consumer reports published by the FTC since 2002. The Identity Theft Act and Assumption Deterrence Act of 1998 led the FTC to establish the Identity Theft Data Clearinghouse in November 1999 to collect identity theft complaints from victims.[11] 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 used consumer reported identity thefts for each state, including Washington D.C. from the years 2002 to 2007 collected from the FTC. Since only annual data are published, we invoked the Freedom of Information Act to request monthly data. We then aggregated the monthly data into semi-annual time periods (producing 612 observations) since this was the smallest time frame for which we expected to see an effect of law. This is an attractive data source because it removes the possibility of inconsistent data collection between states which could lead to erroneous estimations.

However, the data have some limitations. One of which is that it is self-reported, 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. However, to our knowledge, the FTC is the only source for cross-sectional (that is, cross-state) time series data on identity theft. Moreover, in

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

our model, underreporting is problematic only if the reporting pattern changes over time within a state. If the reporting levels change all across the nation then our time dummies should capture it. However, it is conceivable that after the laws are passed, the reporting rates may increase due to more consumer awareness. We discuss how we control for this in later sections.

Other surveys provide some insights into these crimes but they are neither time series nor comprehensive enough (see survey by Bureau of Justice Statistics, Synovate, and Javelin Strategy and Research).[12,13,14]

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 3. In 2007, Arizona had the highest reported identity theft rate of 138 while North Dakota had the lowest, at 28.5.

[Insert Table 3: Identity theft reports, 2002 to 2007]

[Insert Figure 3: Identity theft rate for 2002 to 2007]

These data show identity theft reports increasing at a decreasing rate from 2002 until 2005, after which they decline slightly in 2006 and increase again in 2007. Prior to 2005, only California had adopted the law, but 11 new states adopted the law in 2005[15] 16 in 2006,[16] and 10 more states in 2007.[17] Figure 5 shows the relative changes in reported identity theft rates for four groups: those that adopted in 2005, 2006, 2007, and those that, as of the end of 2007, had not adopted the law (13 states).[18]

[Insert Figure 5: Comparing reported identity theft rates]

The figure illustrates how all trends are increasing at a decreasing rate from 2002 to 2005, after which there is a slight decline in 2006. States that adopted in 2005, 2006 and those without law show a slight increase in 2007, whereas those that adopted in 2007 remain generally unchanged for 2007. Reported identity thefts for states that adopted the law in 2005 are the highest followed by states that adopted in 2007, and 2006. States that had not adopted (as of December 31, 2007) show the lowest overall identity theft rates. The similarity of each of these trends provides some initial insight into what may (or may not) be driving the changes in identity theft reporting.

We also collected other state specific economic, crime and other related data which are described in the next section.

### 4.2 Causes of Identity Theft

Most often, the causes of identity theft are 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

---

[12] 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.

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

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

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

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

[17] Arizona, Hawaii, Kansas, Michigan, New Hampshire, Oregon, Utah, Vermont, Wyoming and Washington D.C.

[18] Alabama, Alaska, Iowa, Kentucky, Maryland, Massachusetts, Mississippi, Missouri, New Mexico, South Carolina, South Dakota, Virginia and West Virginia.

conducted by Javelin Research (2006), 16% reportedly fell within the control of businesses.[19] 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 in Table 4.

[Insert Table 4: Causes of Identity Theft]

Attackers use stolen 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, mortgages, and loans (Givens, 2000). They can use 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.

## 5. DATA ANALYSIS

The first-order effect of the laws could be to reduce the number of breaches. However, recall that the number of breaches reported is affected by law as well: after the laws are passed, firms are forced to disclose. Therefore, analyzing number of breaches is unlikely to provide useful results. From Figure 4, it is apparent that the number of reported breaches has increased, as expected. However, the number of breaches can serve a useful purpose in controlling for awareness bias, which we discuss in more detail later.

[Insert Figure 4: Data breaches from 2002-2007]

### 5.1 Effect of Law on Identity Theft: Basic Model

We now specify our econometric model to analyze how adoption of laws affects the incidences of identity theft. Before we focus our attention on the panel data, we first explore how the state demographics affect identity theft rates. Notice from Table 3 the large variation in identity theft across states. Clearly, identity theft rate varies across states. We therefore employ a simple cross sectional regression for the year 2002. The estimating equation is:

$$\text{idtheft}_s = \beta_0 + \sum \delta_s \text{Economic}_s + \sum \alpha_s \text{Crime}_s + \varepsilon_s \qquad (1)$$

*idtheft* is a normalized variable for identity thefts per 100,000 people in state *s*. $Economic_s$ 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. The CIMIP study (2007) observed that offenders of identity theft tend to have a history of crime. Therefore, we include a $Crime_{st}$ vector that captures both violent (murder, robbery) and property (burglary, motor-vehicle theft) crimes. Further, as shown in Table 4, 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.

This regression should provide insight into how state demographic characteristics are correlated with the identity thefts. 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. Crime data was obtained from the Federal Bureau of Investigations (Uniform Crime Reports) and the FTC. We will discuss all the results in the next section.

[19] 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%.

We now turn to estimating the effect of law on identity theft. To identify the effect of law, we use the panel nature of our data and employ state and time fixed effects. Thus, our basic estimating model has the form:

$$idtheft_{st} = \beta_0 + \beta_1 hasLaw_{st} + \sum \rho_{st} Related_{st} + \sum \delta_{st} Economic_{st} + \sum \alpha_{st} Crime_{st} + \theta_s + \lambda_t + \varepsilon_{st} \quad (2)$$

*s* indexes the state while *t* indexes time (12 time periods). *Idtheft*, as before, is a normalized variable for identity thefts per 100,000 people in state *s* at time *t*. $hasLaw_{st}$ is the dummy variable which is one if the state has adopted the law and zero otherwise. This dummy captures the effect of law on the identity theft rate. The dates of the adoption of data breach notification laws from January 1, 2002 to December 31, 2007 were obtained from state and federal legislation websites. For the purpose of analysis, we are concerned with the date the law became effective rather than the date the law was passed.

$Related_s$ 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.[20] The Fair and Accurate Credit Transactions Act (FACTA)[21] 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.

$Economic_{st}$, and $Crime_{st}$ are same as explained in model (1) above except they are now indexed with state and time. Thus we include economic and crime characteristics of a state at every time period (every 6 months). We do not include demographic controls such as race or age composition because we believe these effects remain relatively constant over our six year time window and will therefore be captured by state fixed effects. Descriptive summary statistics for these variables are provided in Table 5.

$\theta_s$ and $\lambda_t$ are state and time fixed-effects and $\varepsilon_{sy}$ is the familiar error term. This state, time fixed effect model (sometimes known as the difference-in-difference model) is widely used in the literature to examine the effect of a policy intervention (Bertrand, Duflo and Mullainathan 2004). State fixed effects allow us to control for unobserved state specific factors and time dummies allow us to control for time trends. Thus the unbiased effect of *haslaw* can be identified. Regressions are estimated with heteroskedastic robust standard errors clustered-corrected by state.

## 5.2 Extended Model

The basic model in equation (2) estimates the average effect of law. We also extended that model to gain deeper understanding into how law may have differential effects.

*Lagged law*: it is conceivable that the effect of law increases as firms invest in security measures over time. To test this, we introduce three lagged dummies *d1PerOld*, *d2PerOld*, and *d3PerOld*, representing 1 (6 months), 2 (one year) and 3 or more (1.5 years+) periods after the law is adopted, respectively.

*The national effect*: One of the challenges in our data is that when a state enacts the law, it may affect identity thefts in other states because of the residency requirements. Thus the effect of law may diffuse across all states, reducing the power of our test. We use two measures to control this. First, we weight identity theft by interstate commerce activity in 2002 has a proxy for how connected a state is with other states. 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 mis-recorded reports to the degree that the students are out-of-state residents. However, a breach of a

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

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

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), only 35% (181) of identity theft crimes occurred out-of-state.

Second, we interact the *hasLaw* dummy variable with the percentage of all US states that have adopted the law (*Law*PercStatesWLaw*). Now the *haslaw* dummy can be interpreted as the effect of law when no other states have adopted these laws. If the effect of law is significantly diffused then the marginal impact of law may reduce as more and more states have adopted the disclosure laws.

*Differential effect of law across the states*: It is reasonable to think that the effect of the laws would be different across the states. 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 to 2007. High income states are those with average incomes greater than the median ($3,237). We interact high income with the breach law (*Law*HighIncome*). Using data on percent urbanization for each state,[22] 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*).

*Strictness of Law*: In the basic model, we have assumed that all breach disclosure laws are homogenous. In the extended model we relax this assumption and consider that some laws may be stricter if they exhibit the following properties: are acquisition-based (forcing more disclosure from a lower threshold of breach), cover all entities (businesses, data brokers and government institutions), and allow for a private right of action (i.e. class action law suits). Based on the examination of state laws, we classify six states as having stricter laws: California, Hawaii, Illinois, Louisiana, Nevada and Rhode Island. We then interact strictness with the state's adoption of the law (*hasLaw*Strict*) to compare states with strict and non-strict laws.

## 6. RESULTS

### 6.1 Effect of Law on Identity Theft

The results of the regression in Equation (1) (about how the state demographics affect identity theft rates) are shown in Table 6 and suggest that identity theft is highly correlated with population, fraud and both violent and property crime variables. On average, more populous states suffer from higher rate of identity thefts. This may reflect the nonlinear nature of identity theft crime. Other crime related variables are significant though the signs are in different directions. States with higher fraud rate, robbery rates and motor vehicle theft rates have high level of identity thefts.

We now turn to using the full panel dataset. The results of Equation (2) (the basic model) are shown in Table 7. 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. We also report the results of the extended model in Table 7. Thus column 1 of Table 7 has the results of the basic model and we extend this model in column 2 (lagged law), column 3 (weighting the identity theft by state's commerce), and column 4 (interaction of law with other states adopting the law). Columns 3 and 4 control for the national effect. To avoid clutter, we do not report the interaction of law with state specific effects and strictness of law. These effects are statistically and economically insignificant.

All specifications use cluster-corrected standard errors by state and include time dummies for 12 periods though we do not report those estimates to improve readability. Overall, we expect a negative coefficient for all of the law-related variables, indicating that their presence reduces the numbers of identity thefts.

In Specification 1 (column 1), the coefficient of law is -1.129 suggesting that data breach disclosure laws reduce identity thefts by about 1 per 100,000 people. Since the average identity rate was about 69.6 in 2005, this implies that the laws reduced the rate by about 1.6% (1.1/69.6). However, this is not statistically significant.

Specification 2 (the extended model) shows the effect of the lagged adoption of law and suggests that 6 months after adoption, identity theft rate decreases by about 5 per 10 million people but is not statistically

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

significant. Periods of 12 and 18 months after adoption show a stronger negative but still insignificant effect, suggesting that the effect of law is not strong even after 18 months.

The dependent variable in Specification 3 (the extended model) 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 interpretation of the coefficient is unchanged from previous specifications. The coefficient of law is small (-0.592) but now significant at the 5% level. Finally, Specification 4 (the extended model) accounts for interstate transactions by interacting a state's law with the percentage of total states that have adopted the law. This coefficient on law is similarly negative but non-significant (-0.459). The *haslaw* dummy should be interpreted as the effect of law when no other state has passed such law.

As mentioned, we also examined the impact of law in states with higher populations, average income, urbanization and with stricter laws, respectively. With those controls, we similarly found insignificant results. Together, these findings suggest that the laws in higher income and more urban states do not reduce identity theft relative to their complement. Moreover, stricter laws are not found to reduce identity thefts more than weaker ones.

In summary, we find a small effect of law on the incidences of identity thefts. This, in itself does not suggest that the laws are ineffective for there are other dimensions to the effects of law. For example, the laws naturally lead to more disclosures, and it is also conceivable that the laws may not reduce identity thefts but may decrease the economic losses associated with these thefts, or may reduce of the severity of losses from identity thefts. However, we cannot identify these effects from our data.

## 6.2 Awareness Bias

A further consideration of disclosure laws is that they may produce a secondary but conflicting (opposing) effect by increasing consumer awareness, what we call an *awareness bias*. We noted that one of the limitations of our data is that they are self reported and so the passage of law might increase awareness, causing more reporting. This, in turn, will dampen our estimate as explained in Figure 6.

[Insert Figure 6: Awareness Bias]

First, as more consumers are notified of breaches, the number of consumers who will check their credit reports and discover instances of identity theft will increase. Second, as more state-level disclosure laws are passed, they fuel an increase in media attention from data breaches and the threat of identity theft. This may cause more victims from *all forms of identity theft* (not just from data breaches) to report the crime.[23] For example, newspaper and magazine articles often provide recommendations to victims of identity theft by encouraging them to report the incident to law enforcement and the FTC.

Therefore, the net effect of disclosure laws and awareness bias is shown in Figure 7. On one hand, breach laws may result in fewer crimes, but on the other hand the awareness bias may lead to more reporting of crimes. However, note that any increase in reporting due to this phenomenon would cause the regression coefficients of law to be attenuated toward zero. In effect, awareness bias would represent an underestimate or lower bound of the effect of law.

[Insert Figure 7: Downward biased estimates]

As noted earlier, an increase in awareness common to all states (say, from a nationally syndicated news program or nationally circulated online or printed magazine) would be captured in our regression by time dummies.

[23] In July 2006, the OMB (Office of Management and Budget) issued a requirement to all government agencies that they report any security incidents (including breaches) involving PII. During a conference in October 2007, Karen Evans, administrator of the Office of Electronic Government and Information Technology at the OMB claimed that the number of reports has increased to about 30 incidents a day. She further commented that the increased level of reporting "reflects increased market awareness."

One possible control for awareness bias could be the number of disclosed data breaches as described earlier. As media stories of state breaches are reported, they increase awareness of the breach, and often include information on how consumers can protect themselves against the consequences of the breach, and how they should respond in the event of becoming a victim of identity theft. Indeed, a very common recommendation is for consumers to file reports with law enforcement and to the FTC (via the 800 telephone number or website). The media attention due to a local or state-wide breach may result in more reporting and so controlling for these breaches may allow us to obtain better estimates of the true effect of law.

We analyzed each breach and categorized it as either a national or state-level breach. National breaches were those that affected consumers in multiple states (for instance the Choicepoint breach of 2005 or the Veterans affairs breach of 2006). State breaches are those that affect consumers of a single state only. For instance, breaches in high schools, colleges, hospitals or state government agencies. Observations were dropped in cases where the scope of affected consumers was unknown or ambiguous, or when a breach affected consumers in more than one state. Of the 773 breaches, 521 were classified as state-level breaches. Panel data were thus created using the number of breaches per state, per 6 month period from 2002 to 2007. The estimating model then becomes:

$$idtheft_{st} = \beta_0 + \beta_1 hasLaw_{st} + \beta_2 breaches_{st} + \sum \rho_{st} Related_{st} + \sum \delta_{st} Economic_{st} + \sum \alpha_{st} Crime_{st} + \theta_s + \lambda_t + \varepsilon_{st} \quad (3)$$

The other variables remain unchanged from the previous section but we now include breach data that varies by state and time. The results are shown in Table 8 where we report the same specifications as in Equation (2).

As expected, after proxying for increased awareness through number of reported breaches, the coefficients of the effect of law in all specifications are now larger in magnitude. Moreover, the coefficients of the effect of law in Specifications 5 (-1.279) and 7 (-0.729) are now statistically significant at the 10% and 5% level, respectively. Using the average identity theft rate of 69.6 in 2005, the estimate of 1.279 suggests that, on average, adoption of data breach disclosure laws reduces the identity theft rate by 1.8% (1.28/69.6).

Again, we examined the impact of law in states with larger populations, higher average income, urbanization and with stricter laws. We found no statistically significant evidence indicating that the laws were more effective in any of these four conditions.

### 6.3 Endogeneity of the law

Another consideration for our analysis is the endogeneity of law. It may be argued that the laws are systematically adopted because of higher rates of identity theft within a state. Since the laws are adopted when identity theft levels have reached the peaks, we may find a spurious and positive effect of law (i.e. laws reduce the rates) when there is none. Conversations with privacy and data breach lawyers confirm our exogeneity claim that these disclosure laws are not adopted because of identity theft, but due to other factors such as: state-level lobbying by privacy advocacy and corporate interest groups, the political motivation of state legislators (looking to improve their reputation or by making "good law"), or particular "shocks" to the system.

All of these factors suggest exogeneity of law, with the possible exception of the last. A "shock" in this context would imply that a state adopted the law because of a sudden surge of identity thefts in a previous period. To be clear, we find no evidence that disclosure laws were adopted specifically because of a sudden rise in identity theft crimes, as shown in Figure 8.[24]

[Insert Figure 8: Changes in identity theft for states with and without law]

If the laws were, indeed, endogenous, we would expect to see an increased identity theft rate both: a) immediately before adoption of the law, and b) compared to states without the law. We see no such systematic increase for states that adopted the law. In fact, the changes in these groups very closely match the trend for states without the law.

[24] For example, the 2003 data point for states without the law is the percent change of the average identity theft rate in 2003 over 2002.

### 6.4 Sampling bias

From 2004 to 2006, the FTC (FTC, 2007) identifies the 18-29 year old cohort consistently reporting more identity thefts relative to those aged 60 and over who report less. 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 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 sampling bias. [25] It should be noted that our results are robust as long as the consumer segments reporting to FTC do not change over time. However, the results should be interpreted as being specific to the segment which is reporting more frequently than to those who do not.

## 7. DISCUSSION

We believe the results of Equation (3) speak to the deterrent effect of data breach disclosure laws and therefore it may be useful to provide context for our estimates by examining the effect of other treatments (e.g. law) in other studies.

Table 9 presents a comparison of ranges of estimates for various criminal laws and disclosure policies on relevant outcome measures. From this limited sample, the effects of treatments range from -8% to +15% with an overall average of -0.5%. This places our result of -1.8% well within the norm of this sample.

[Insert Table 9: Comparison of treatment effects]

We can also provide one estimate of the potential savings to consumers. Recall that the average amount stolen from consumers in 2005 was $6,383 (Javelin, 2006). With 8.9 M estimated victims in 2005, a 1.8% reduction in identity thefts would translate to a savings of about $1 billion (8.9 M* 0.018 * $6,383). We stress that care must be taken when interpreting these results. These savings are shown merely to provide context and should not be interpreted literally.

Further, the lack of stronger significant findings may be due to a number of factors:

One explanation is that the laws could simply not be very 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. However, it is also possible that our data limitations prohibit us from identifying the effect.

While reported crime 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. Nevertheless, we tried to control for some sources of bias, and we believe the data collected and published by the FTC is currently the best source of identity theft data.

It is conceivable that the effect of laws is not state specific but diffused across the nation which limits the power of our analysis. While we have tried to control for these effects by weighing the data and by interacting with other states, it is possible that the effect is dampened.

That said, we believe our analysis used the best available data and controls for various limitations as best as possible. State and time fixed effects are also very effective in controlling unobserved state and time trends.

## 8. 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 a very strong effect that the laws reduce the

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

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.

## 8.1 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.[26] 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.

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."

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 a consumer's time and financial costs 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. This also offers interesting research opportunities. If such data were to be available, it would provide alternative ways to evaluate the impact of these laws.

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 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.

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

## 8.2 Firm losses and incentives

Firms may also suffer from optimism bias. 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.[27]

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.[28] 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.[29]

## 8.3 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 sampling and awareness 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.

# 9. CONCLUSION

As information security and privacy concerns rise in society, we will increasingly see legislation as an instrument. Regulations tend to generate policy debates, consumer concerns and significant lobbying. Unfortunately, many times regulations are passed (or not passed) without measuring and analyzing their effects. In this paper, we investigate the effects of increasingly popular, though contentious data disclosure laws, on incidences of identity thefts. Despite US states having adopted these laws over last five years, we have not seen any empirical work that examines the efficacy of these laws. Using panel data from 2002 to 2007 for 50 states (plus Washington D.C.), we conduct a rigorous empirical analysis to examine if the laws have reduced the incidences of identity thefts. We find only a marginal effect of law. We estimate that the passage of law has reduced identity theft rate by about 2%. We also perform various robustness checks and control for various factors when analyzing the effect.

Clearly, it appears that the effectiveness of data breach disclosure laws relies on actions taken by both firms and consumers. Certainly firms must improve their controls, but regardless, once notified consumers must themselves take responsibility to reduce their own risk of identity theft – something which only a minority appears to be doing. It may be that only with time we see more firms internalize the costs, more consumers respond to the risks, and the victimization rates decline.

The goal of this study is to not just highlight these results, but also to draw attention of IS and information security research community to an increasingly important policy issue. We need better data collection, measurements and more studies that can inform policy makers, consumer groups and industry participations regarding the role of regulations in this domain. Otherwise, policy decisions will be made by partisan debates, lobbying efforts and unmeasured and conflicting outcomes.

---

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

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

[29] 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.

# 10. APPENDIX

## 10.1 Figures

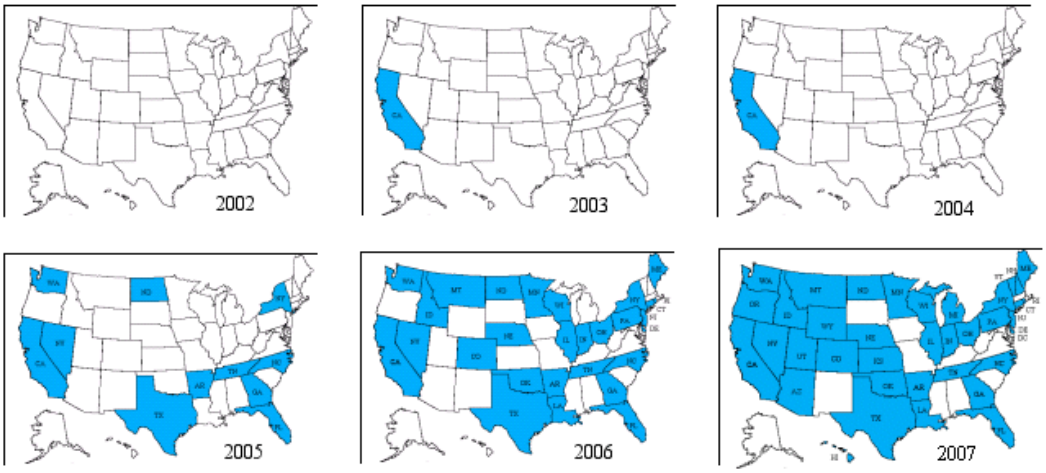


**Figure 1: Adoption of breach notification laws from 2002 to 2007**

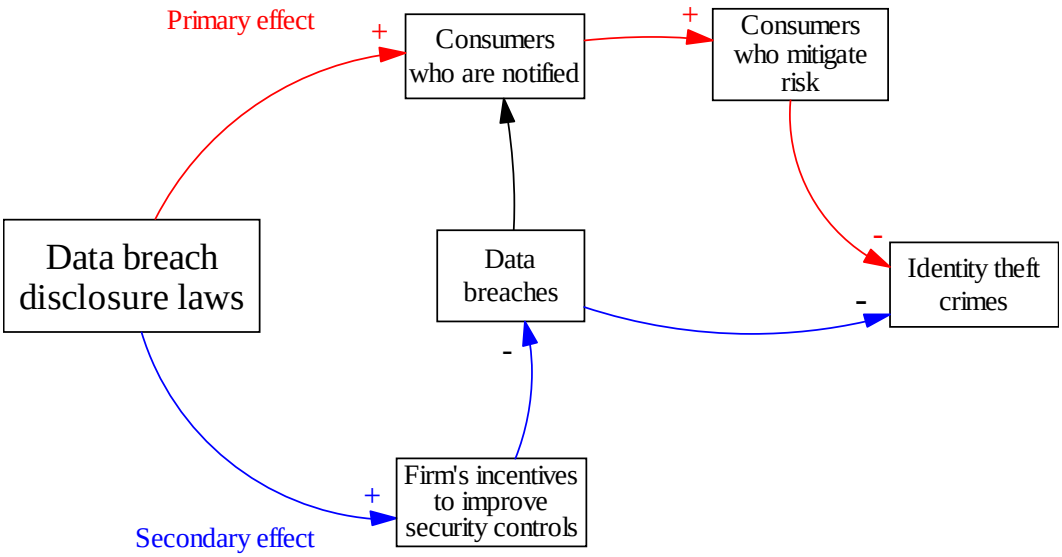


**Figure 2: Two effects of data breach disclosure law**

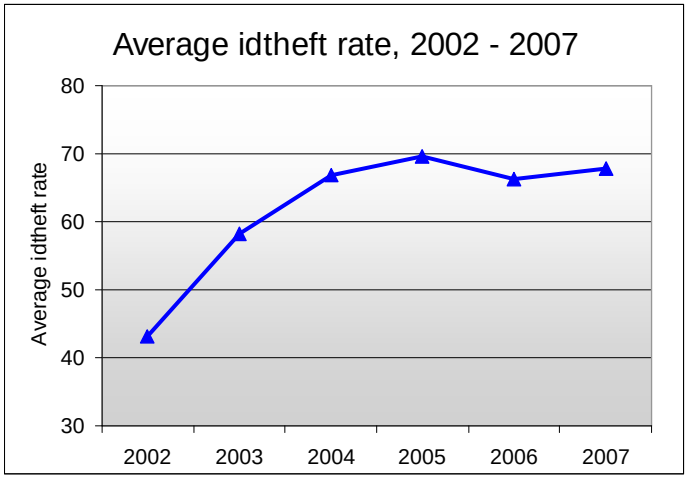


**Figure 3: Identity theft rate for 2002 to 2007**

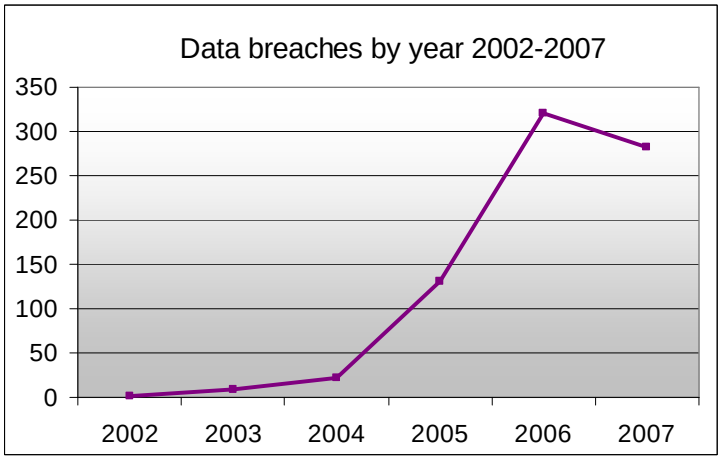


**Figure 4: Data breaches from 2002-2007**

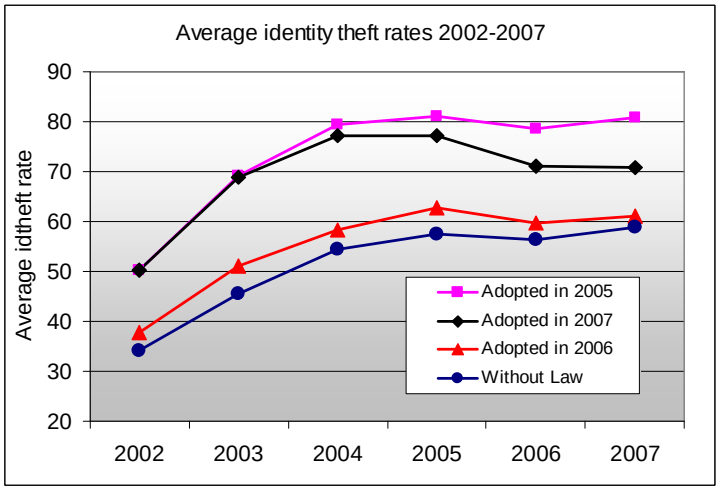


**Figure 5: Comparing reported identity theft rates**

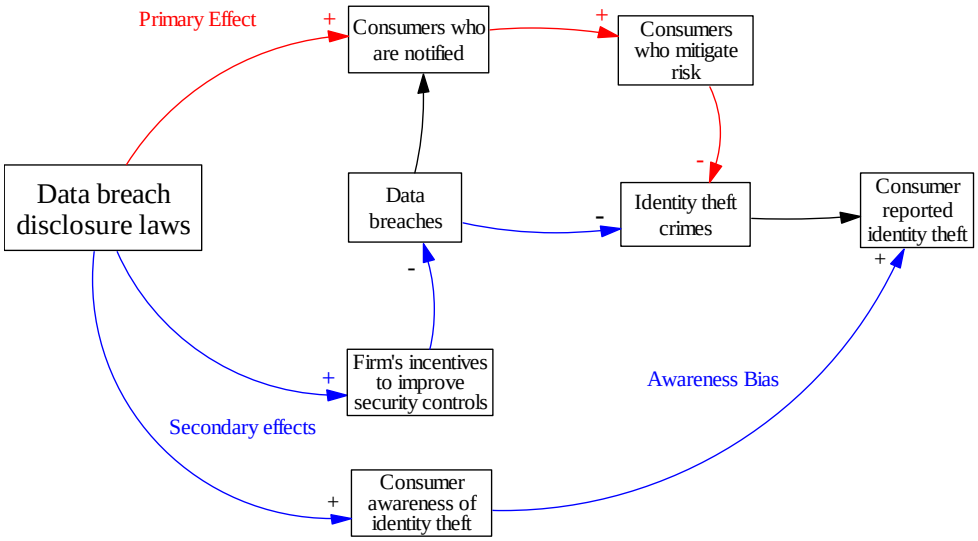


**Figure 6: Awareness Bias**

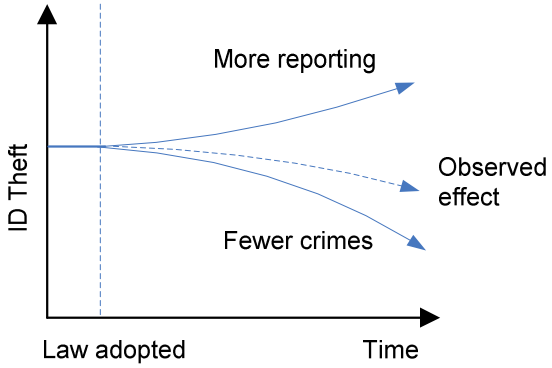


**Figure 7: Downward biased estimates**

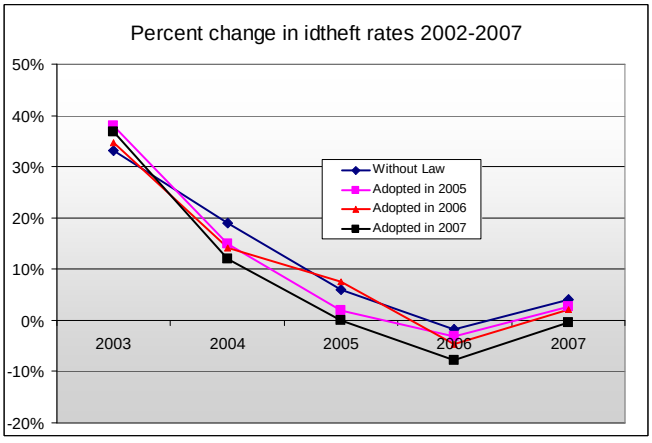


**Figure 8: Changes in identity theft for states with and without law**

## 10.2 Tables

**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 | |

**Table 2: Adoption of law by state, 2002 to 2007**

| State | Adoption Date | 2002 | | 2003 | | 2004 | | 2005 | | 2006 | | 2007 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 | P9 | P10 | P11 | P12 |
| Alabama | | | | | | | | | | | | | |
| Alaska | | | | | | | | | | | | | |
| Arizona | 01/01/07 | | | | | | | | | | | X | X |
| Arkansas | 03/31/05 | | | | | | | X | X | X | X | X | X |
| California | 07/01/03 | | | | X | X | X | X | X | X | X | X | X |
| Colorado | 09/01/06 | | | | | | | | | | X | X | X |
| Connecticut | 01/01/06 | | | | | | | | | X | X | X | X |
| Delaware | 06/28/05 | | | | | | | | X | X | X | X | X |
| Florida | 07/01/05 | | | | | | | | X | X | X | X | X |
| Georgia | 05/05/05 | | | | | | | X | X | X | X | X | X |
| Hawaii | 01/01/07 | | | | | | | | | | | X | X |
| Idaho | 07/01/06 | | | | | | | | | | X | X | X |
| Illinois | 01/01/06 | | | | | | | | | X | X | X | X |
| Indiana | 06/30/06 | | | | | | | | | | X | X | X |
| Iowa | | | | | | | | | | | | | |
| Kansas | 01/01/07 | | | | | | | | | | | X | X |
| Kentucky | | | | | | | | | | | | | |
| Louisiana | 01/01/06 | | | | | | | | | X | X | X | X |
| Maine | 01/31/06 | | | | | | | | | X | X | X | X |
| Maryland | | | | | | | | | | | | | |
| Massachusetts | | | | | | | | | | | | | |
| Michigan | 07/02/07 | | | | | | | | | | | | X |
| Minnesota | 01/01/06 | | | | | | | | | X | X | X | X |
| Mississippi | | | | | | | | | | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Missouri | | | | | | | | | | | | | |
| Montana | 03/01/06 | | | | | | | | | X | X | X | X |
| Nebraska | 07/14/06 | | | | | | | | | | X | X | X |
| Nevada | 10/01/05 | | | | | | | | X | X | X | X | X |
| New Hampshire | 01/01/07 | | | | | | | | | | | X | X |
| New Jersey | 01/01/06 | | | | | | | | | X | X | X | X |
| New Mexico | | | | | | | | | | | | | |
| New York | 12/08/05 | | | | | | | | X | X | X | X | X |
| North Carolina | 12/01/05 | | | | | | | | X | X | X | X | X |
| North Dakota | 06/01/05 | | | | | | | X | X | X | X | X | X |
| Ohio | 02/17/06 | | | | | | | | | X | X | X | X |
| Oklahoma | 06/08/06 | | | | | | | | | X | X | X | X |
| Oregon | 10/01/07 | | | | | | | | | | | | X |
| Pennsylvania | 06/30/06 | | | | | | | | | | X | X | X |
| Rhode Island | 03/01/06 | | | | | | | | | X | X | X | X |
| South Carolina | | | | | | | | | | | | | |
| South Dakota | | | | | | | | | | | | | |
| Tennessee | 07/01/05 | | | | | | | | X | X | X | X | X |
| Texas | 09/01/05 | | | | | | | | X | X | X | X | X |
| Utah | 01/01/07 | | | | | | | | | | | X | X |
| Vermont | 01/01/07 | | | | | | | | | | | X | X |
| Virginia | | | | | | | | | | | | | |
| Washington | 07/24/05 | | | | | | | | X | X | X | X | X |
| West Virginia | | | | | | | | | | | | | |
| Wisconsin | 03/31/06 | | | | | | | | | X | X | X | X |
| Wyoming | 07/01/07 | | | | | | | | | | | | X |
| D.C. | 07/01/07 | | | | | | | | | | | | X |
| Total adopters | | 0 | 0 | 0 | 1 | 1 | 1 | 4 | 12 | 23 | 28 | 34 | 38 |
| Percent adopted | | 0 | 0 | 0 | 2 | 2 | 2 | 8 | 24 | 45 | 55 | 67 | 75 |

**Table 3: Identity theft reports, 2002 to 2007**

| Year | Average | Stdev | Min | Max | Total | Idtheft Rate | % Change |
|---|---|---|---|---|---|---|---|
| **2002** | 3,040 | 5,019 | 81 | 30,782 | 155,028 | 43.1 | |
| **2003** | 4,079 | 6,526 | 127 | 39,500 | 208,033 | 58.3 | 34.2% |
| **2004** | 4,705 | 7,464 | 179 | 43,900 | 239,960 | 66.9 | 15.3% |
| **2005** | 4,874 | 7,621 | 158 | 45,180 | 248,591 | 69.6 | 3.6% |
| **2006** | 4,694 | 7,178 | 178 | 41,415 | 239,391 | 66.4 | -3.7% |
| **2007** | 4,929 | 7,608 | 182 | 44,020 | 251,385 | 67.8 | 5.0% |

**Table 4: 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% |

**Table 5: Descriptive statistics**

| Variable | Mean | Std. Dev | Min | Max |
|---|---|---|---|---|
| Identity theft rate | 31.00 | 14.13 | 5.67 | 84.87 |
| Has data breach law | 0.23 | 0.42 | 0 | 1 |
| Has FACTA | 0.50 | 0.50 | 0 | 1 |
| Has Credit Freeze Law | 0.17 | 0.38 | 0 | 1 |
| d1PerOld (6 months old) | 0.06 | 0.23 | 0 | 1 |
| d2PerOld (12 months old) | 0.05 | 0.21 | 0 | 1 |
| d3PerOld (18 months old) | 0.07 | 0.25 | 0 | 1 |
| State GDP per capita | 4098.89 | 1569.72 | 2347.46 | 15947.69 |
| Income per capita | 3337.91 | 609.96 | 2137.21 | 6192.59 |
| Unemployment rate | 4.97 | 1.14 | 2.18 | 8.55 |
| Ln(population) | 15.06 | 1.04 | 13.11 | 17.41 |
| Fraud rate | 62.55 | 24.10 | 16.80 | 249.68 |
| Murder rate | 5.34 | 5.20 | 0.50 | 46.40 |
| Robbery rate | 116.88 | 96.33 | 6.80 | 706.80 |
| Burglary rate | 701.35 | 230.70 | 309.30 | 1221.50 |
| Motor vehicle theft rate | 379.45 | 245.51 | 85.93 | 1776.50 |
| Breaches | 0.85 | 1.83 | 0 | 15 |

**Table 6: Effect of law on identity theft (Equation (1))**

Dep var: identity theft rate for 2002

| | |
|---|---|
| State GDP per capita | -0.000 |
| | (0.001) |
| Income per capita | -0.002 |
| | (0.002) |
| Unemployment rate | 0.866 |
| | (0.551) |
| Ln(population) | 3.312*** |
| | (0.705) |
| Fraud rate | 0.343*** |
| | (0.059) |
| Murder rate | -0.572** |
| | (0.250) |
| Robbery rate | 0.052*** |
| | (0.018) |
| Burglary rate | -0.008** |
| | (0.003) |
| Motor vehicle theft rate | 0.024*** |
| | (0.004) |
| Constant | -47.317*** |
| | (10.617) |
| Observations | 102 |
| R-squared | 0.87 |

Standard errors in parentheses,

*** p<0.01, ** p<0.05, * p<0.1

**Table 7: Effect of law on identity theft (Equation (2))**

| Dep var: idtheft rate | (1) Basic | (2) Lagged Law | (3) Weighted | (4) National |
|---|---|---|---|---|
| Has breach law | -1.129 | | -0.592* | -0.906 |
| | (0.705) | | (0.344) | (0.938) |
| 6 month old law | | 0.052 | | |
| | | (0.666) | | |
| 12 months old law | | -0.927 | | |
| | | (0.837) | | |
| 18 months old law | | -0.184 | | |
| | | (0.970) | | |
| Law * % states with law | | | | -0.459 |
| | | | | (1.779) |
| Has FACTA | 0.375 | 0.349 | 0.744* | 0.365 |
| | (0.748) | (0.753) | (0.437) | (0.752) |
| Has credit freeze law | 0.821 | 0.515 | 0.877 | 0.828 |
| | (0.936) | (0.881) | (0.593) | (0.940) |
| State GDP per capita | 0.001 | 0.001 | 0.002 | 0.001 |
| | (0.002) | (0.002) | (0.001) | (0.002) |
| Income per capita | -0.002 | -0.002 | -0.003 | -0.002 |
| | (0.003) | (0.003) | (0.002) | (0.003) |
| Unemployment rate | 0.292 | 0.300 | -0.295 | 0.293 |
| | (0.523) | (0.522) | (0.256) | (0.523) |
| Ln(population) | 52.485** | 49.136** | 31.996** | 52.566** |
| | (24.856) | (24.029) | (13.288) | (24.865) |
| Fraud rate | -0.043*** | -0.041*** | -0.026*** | -0.044*** |
| | (0.014) | (0.014) | (0.008) | (0.015) |
| Murder rate | 0.719*** | 0.697*** | 0.323* | 0.720*** |
| | (0.236) | (0.238) | (0.164) | (0.237) |
| Robbery rate | -0.085*** | -0.080*** | -0.041*** | -0.085*** |
| | (0.027) | (0.026) | (0.013) | (0.027) |
| Burglary rate | 0.016* | 0.014 | 0.010* | 0.016* |
| | (0.009) | (0.009) | (0.005) | (0.009) |
| Motor vehicle theft rate | 0.006 | 0.007 | -0.002 | 0.006 |
| | (0.010) | (0.010) | (0.005) | (0.010) |

| | | | | |
|---|---|---|---|---|
| Constant | -777.398** | -726.239** | -471.873** | -778.617** |
| | (373.522) | (360.907) | (201.562) | (373.656) |
| Observations | 612 | 612 | 612 | 612 |
| R-squared | 0.79 | 0.79 | 0.65 | 0.79 |

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

**Table 8: Effect of law on identity theft (Equation (3))**

| | (5) | (6) | (7) | (8) |
|---|---|---|---|---|
| Dep var: idtheft rate | Basic | Lagged Law | Weighted | National |
| Has breach law | -1.279* | | -0.729** | -0.955 |
| | (0.701) | | (0.353) | (0.966) |
| 6 months old law | | -0.029 | | |
| | | (0.667) | | |
| 12 months old law | | -1.087 | | |
| | | (0.847) | | |
| 18 months old law | | -0.428 | | |
| | | (0.983) | | |
| Law * % states with law | | | | -0.673 |
| | | | | (1.820) |
| Breaches | 0.177* | 0.157* | 0.161*** | 0.180** |
| | (0.090) | (0.088) | (0.041) | (0.087) |
| Has FACTA | 0.326 | 0.306 | 0.699 | 0.310 |
| | (0.756) | (0.763) | (0.448) | (0.759) |
| Has credit freeze law | 0.897 | 0.570 | 0.946 | 0.909 |
| | (0.932) | (0.882) | (0.595) | (0.937) |
| State GDP per capita | 0.002 | 0.002 | 0.002 | 0.002 |
| | (0.002) | (0.002) | (0.001) | (0.002) |
| Income per capita | -0.002 | -0.002 | -0.003 | -0.002 |
| | (0.003) | (0.003) | (0.002) | (0.003) |
| Unemployment rate | 0.376 | 0.381 | -0.219 | 0.377 |
| | (0.525) | (0.524) | (0.255) | (0.525) |
| Ln(population) | 54.032** | 50.644** | 33.405** | 54.169** |
| | (24.667) | (23.760) | (13.009) | (24.663) |
| Fraud rate | -0.043*** | -0.041*** | -0.025*** | -0.043*** |

| | | | | |
|---|---|---|---|---|
| | (0.014) | (0.014) | (0.008) | (0.015) |
| Murder rate | 0.759*** | 0.733*** | 0.359** | 0.761*** |
| | (0.230) | (0.235) | (0.161) | (0.231) |
| Robbery rate | -0.086*** | -0.081*** | -0.042*** | -0.085*** |
| | (0.027) | (0.026) | (0.013) | (0.027) |
| Burglary rate | 0.015* | 0.014 | 0.009** | 0.015* |
| | (0.009) | (0.009) | (0.005) | (0.009) |
| Motor vehicle theft rate | 0.006 | 0.007 | -0.002 | 0.006 |
| | (0.010) | (0.010) | (0.005) | (0.010) |
| Constant | -800.920** | -749.408** | -493.285** | -802.989** |
| | (370.412) | (356.617) | (197.087) | (370.343) |
| R-squared | 0.79 | 0.79 | 0.66 | 0.79 |

Robust standard errors in parentheses,

*** p<0.01, ** p<0.05, * p<0.1

**Table 9: Comparison of treatment effects**

| Research | Treatment | Outcome measure (Result) |
|---|---|---|
| Donohue (2004) | Right-to-Carry laws | Violent crime rate: -3% to +4%<br>Murder rate: -8% to +3%<br>Motor vehicle theft rate: -7% to +15%<br>Property crime rate: 0% to +10% |
| Epple and Visscher (1984) | Coast guard monitoring | Oil spill frequency: +2.1%<br>Oil spill volume: - 3.1% |
| Cohen (1987) | Coast guard monitoring | Oil spill frequency: -2%<br>Oil spill volume: -1.7% |
| Hamilton (1995) | Disclosure of toxic release (TRI) | Stock price: -0.3% |
| Acquisti, Telang and Friedman (2006) | Disclosure of security breach | Stock price: -0.6% |

Acknowledgements:

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. Rahul Telang and Sasha Romanosky also wish to acknowledge the generous financial support of NSF (National Science Foundation) via CAREER grant CNS-0546000.

Sasha Romanosky is a PhD student at the Heinz School, Carnegie Mellon University and his research field is the economics of information security. He holds a Bachelor of Science degree in Electrical Engineering from the University of Calgary, Canada. He holds the CISSP security certification and has been working with internet and security technologies for over 10 years, predominantly within the financial and e-commerce industries at companies such as Morgan Stanley and eBay. He is coauthor of "J2EE Design Patterns Applied" and "Security Patterns: Integrating Security and Systems Engineering" and has published other works on information security. Sasha developed FoxTor, the Firefox extension used for anonymous web browsing. He is also co-author of the Common Vulnerability Scoring System (CVSS), an open framework for scoring computer vulnerabilities that is widely adopted by many organizations including the NIST S-CAP project and the Payment Card Industry data security standard (PCI/DSS).

Rahul Telang is an Associate Professor of Information Systems and Management at the Heinz School, Carnegie Mellon University. He received his Ph.D. in Information Systems from the Tepper School of Business at Carnegie Mellon University in 2002. Dr Telang's key research field is the economics of Information security and piracy. He has done extensive empirical as well as analytical work on disclosure issues surrounding software vulnerabilities, software vendors' incentives to provide quality etc. He also received the prestigious National Science Foundation CAREER award for his research in economics of information security. He has also done extensive work on piracy. His work on the used book market has been reported in The New York Times among other media outlets. His dissertation won the William W. Cooper Doctoral Dissertation Award. His research has been published in leading journals including Management Science, Information Systems Research, Journal of MIS, and Journal of Marketing Research. He is on the editorial board of Management Science and Information Systems Research.

Alessandro Acquisti is an Assistant Professor of Information Technology and Public Policy at the H. John Heinz III School of Public Policy and Management, Carnegie Mellon University. His current research focuses primarily on the economics and behavioral economics of privacy and information security. His research in these areas has been disseminated through journals (including Marketing Science, IEEE Security & Privacy, and Rivista di Politica Economica); edited books ("Digital Privacy: Theory, Technologies, and Practices." Auerbach, 2007); book chapters; and leading international conferences. Alessandro has received national and international awards, including the 2005 PET Award for Outstanding Research in Privacy Enhancing Technologies and the 2005 IBM Best Academic Privacy Faculty Award. His research has been featured on outlets such as NBC, NPR, the Washington Post, and the New Scientist.

## 11. 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,” Management Science, 54(4), pages 642-656, 2008.

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,

Bertrand, M., Duflo, E., and Mullainathan, S., "How Much Should We Trust Differences-in-Differences Estimates?," The Quarterly Journal of Economics, MIT Press, vol. 119(1), pages 249-275, February, 2004.

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.

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).

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, 27, April, 29-59, 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.

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.

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.

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.

Li, P. and Rao, H. R., “An examination of private intermediaries' roles in software vulnerabilities disclosure,” Information Systems Frontiers 9, 5 (Nov. 2007), 531-539.

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.

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.

Telang, R., Wattal, S., “An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price”, IEEE Transactions on Software Engineering paper, 33 (8), 544-557, 2007.

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.

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.