TECHNOLOGY POLICY INSTITUTE

Studying the Global Information Economy

"An Economic Analysis of Notification Requirements for Data Security Breaches."

Thomas M. Lenard and Paul H. Rubin

July 2005

1747 PENNSYLVANIA AVENUE NW ▫ SUITE 850 ▫ WASHINGTON, D.C. 20006
PHONE: 202.828.4405 ▫ E-MAIL: info@techpolicyinstitute.org ▫ WEBSITE: www.techpolicyinstitute.org

THE PROGRESS & FREEDOM FOUNDATION

Progress on Point

Release 12.1 2 July 2005 Periodic Commentaries on the Policy Debate

AN ECONOMIC ANALYSIS OF NOTIFICATION REQUIREMENTS FOR DATA SECURITY BREACHES

By Thomas M. Lenard and Paul H. Rubin*

I. INTRODUCTION AND SUMMARY

Congress and the states are moving rapidly to enact new legislation in the wake of a series of high-profile data security breaches by both private and public institutions. [1] Bills have been introduced that would impose a variety of obligations on both businesses and public-sector entities in the event of a security breach, and provide remedies for individuals whose personal information was acquired by an unauthorized party. A major component of all the legislative proposals is a requirement that consumers be notified when a security breach occurs that might compromise their confidential data.

In 2003, California became the first state in the nation to enact a security breach statute .[2] Indeed, the California notification requirement was responsible for the initial publicity surrounding a security breach by information broker ChoicePoint , and the subsequent demand for further legislation. At the present time, thirteen states have security breach legislation in place.

Press accounts and statements from various experts give the impression that identity theft and related frauds are on the rise (Fountain, 2005). For example , the preamble to the California security breach statute states that " [i]dentity theft is one of the fastest growing crimes committed in California." But while identity theft is clearly a major problem, the data do not show that it has been increasing over time.

The most comprehensive data on identity theft and its costs are from a survey commissioned by the Federal Trade Commission and carried out by Synovate in 2003. This analysis was updated for 2004 by Javelin (2005). Virtually all the results, including incidence of identity theft and costs to victims, are about the same (not statistically

---

* Thomas Lenard is senior fellow and vice president for research at The Progress & Freedom Foundation. Paul Rubin is Samuel Candler Dobbs Professor of Law and Economics at Emory University and adjunct fellow at PFF. This paper reflects the views of the authors and not their respective institutions.

1 In addition to the ChoicePoint security breach, there have been major security breaches involving DSW Shoe Warehouse, Boston College and several other universities, Polo Ralph Lauren, Ameritrade and CardSystems.

2 Bill Number 700, available at http://www.leginfo.ca.gov/pub/01- 02/bill/asm/ab_0651-0700/ab_700_bill_20020929_chaptered.html

different) in the two surveys, indicating that fears of identity theft being a rapidly growing problem are exaggerated.[3]

The Synovate and Javelin surveys show that the costs of identity theft and related crimes were essentially constant over the last two years for which data are available. Other data suggest these costs have been decreasing over time. Estimates by Nilson show the total costs of credit card fraud to issuers decreased from $882 million in 2003 to $788 million in 2004—a 10-percent decline (Nilson Report, 2005). Moreover, over a longer period—1992 to 2004—the Nilson Report found that the costs of these frauds have decreased, from $0.157 to $0.047 per $100 in credit card sales.[4] This is not surprising, despite the press accounts, because credit card firms are continually updating and improving levels of security (Bank and Clark, 2005; Pacelle, 2005). The Nilson Report also indicates that fraudulent charges are lower as a percentage of credit card use in the U.S. than in the rest of the world; for example, credit card payments in the U.S. are three times the U.K. level, as compared with fraudulent charges, which are only about 1.2 times the U.K. level.

This paper addresses a number of interrelated issues concerning whether a notification requirement would be in the best interests of consumers and what form it should take:

- Does the private market provide adequate incentives for firms both to secure their data and to provide notice to consumers in the event of a breach?

- Is there reason to believe a notification requirement will yield benefits greater than costs?

- In light of the benefit-cost analysis, how should a notification mandate be structured?

- If there is a requirement, should it be at the state level or should federal law preempt state laws in this area?

Our major conclusions are:

- The annual costs of identity theft and related frauds are $55 billion, $50 billion of which are borne directly by businesses, including banks, credit card issuers and merchants. Firms also suffer large losses in stock value when security is breached. These factors provide strong incentives for companies to spend money on data security.

---

3 The actual incidence of identity theft of all forms decreased from 4.7 percent of the adult population to 4.25 percent, but this difference was not statistically significant.

4 This represents costs to card issuers, and so is not comparable to the FTC numbers, which represent total costs to all businesses and consumers.

- While it is unclear whether firms have adequate incentives to notify compromised consumers, the issue is an empirical one: do the benefits of notification outweigh the costs?

- The expected benefits to consumers of a notification requirement are extremely small—on the order of $7.50 to $10 per individual whose data have been compromised. This is because (1) most cases of identity theft do not involve an online security breach; (2) only a very small percentage of individuals compromised by security breaches—perhaps 2 percent—actually become victims of a fraud; (3) most of these are victims of fraudulent charges on their existing credit accounts, for which they have very limited liability, rather than victims of true identity theft; and, (4) even a well-designed notification program will only eliminate about 10-20 percent of the expected costs.

- Because a notification mandate is dubious on benefit-cost grounds, it should be targeted carefully. Firms should be able to determine which customers are most at risk and tailor notice to those individuals , perhaps in cooperation with the FTC. Encrypted data should be exempt from notice, because it is less likely to be used for fraudulent purposes.

- Federal preemption of state notification laws will reduce compliance costs and improve the benefit-cost balance. A true federalist approach is not possible with markets and firms that are national, and even international, in scope. Firms will tend to comply with a single set of rules. In the absence of a preemptive federal statute, they will comply with the most stringent set of state regulations , which will in effect "preempt" other state regulations.

II. THE COSTS OF SECURITY BREACHES

The FTC estimates that ten million people —or about 4.6 percent of the adult population—are victims of some form of identity theft annually. The estimated out -of-pocket costs of this identity theft are about $55 billion annually, of which about $50 billion are borne by businesses and $5 billion by consumers.

There are two categories of identity theft. Misuse of an existing credit card or other account—i.e., charging items on someone else's account—accounts for two thirds of the total number of incidents . The remaining third consists of opening up new accounts in another person's name and related frauds. This latter category—which corresponds more closely to true identity theft—is substantially more costly to both businesses and individuals . Victims of this type of identity theft incur substantial monetary and time costs attempting to clear up their damaged credit records. In this paper, we follow the convention of including both types of fraud under the rubric of identity theft.

Estimates of the costs of identify theft based on the FTC data are summarized in Table 1. The FTC estimates the average cost to business of new and existing account

fraud is $10,200 and $2,100, respectively. The weighted average cost of an incident is about $4,800.

Table 1: Costs of Identity Theft			
	New Account Fraud	Existing Account Fraud	Total
Incidence (last year)	1.5%	3.1%	4.6%
Weight	0.326	0.674	1.00
Cost to businesses	$10,200	$2,100	$4,800*
Cost to Individuals	$1,180	$160	$500*
Time spent by individuals	60 hrs.	15 hrs.	30 hrs.*
Cost of time @ $15 per hour	$900	$225	$450*
Total cost to individuals	$2,080	$385	$950*

* Weighted averages of new and existing account fraud (totals are rounded).
Source: Computed from Federal Trade Commission (2005), Identity Theft Survey Report, Synovate, September, available on the FTC website.

The cost to individuals of a new account fraud is $1,180 and 60 hours of time. Using $15 per hour as the average wage rate (value of time) (Bureau of Labor Statistics, 2005), this yields a time cost of $900 and a total cost of $2,080. A similar calculation for existing account fraud yields a total cost per incident of $385. The weighted average cost for all types of incidents is $950. Since the incidence of all forms of identity theft is 4.6 percent, the expected cost to the average consumer is about $50. As discussed below, however, any notification requirement will save consumers considerably less than this amount.

III. MARKET RESPONSES

A. Security

As just discussed, the FTC study found that the costs to businesses of identity theft are about 10 times the costs to individuals. The prospect of reducing a $50-billion loss means that the businesses involved—the credit card companies, the banks, merchants and others—should have a strong incentive to invest in data security.

These costs are reflected in the large stock market losses suffered by irms victimized by security breaches. Garg et al (2003) found that firms victimized by a security breach involving theft of credit card information suffered a stock market loss of 9.3 percent on the first day the breach was announced, increasing to 14.9 percent over

three days. This cost is quite large—three to five times the amount found in similar studies for other classes of events.[5] Most breaches involving other types of data did not exhibit significant stock market effects. Similarly, Campbell et al. (2003) found that there was no significant effect of breaches that did not involve data security, but that breaches associated with violations "such as customer databases" did lead to significant losses in stock value. It is important to note that these results are from a period before any consumer notification was required. Nonetheless, information about the breach became public—perhaps as a result of securities regulatory requirements—and markets reacted accordingly. Thus, even without any laws mandating notice to consumers, firms have had a very strong incentive to avoid data security breaches because the market penalizes them severely.

This is reflected in the behavior of the credit card companies, which continue to devise new and better security systems as they compete to sign up merchants (Bank and Clark, 2005; Pacelle, 2005; Morriss and Korosec, 2005). While the primary purpose of increasing security is to reduce the costs of fraud to businesses, the costs to consumers are also reduced . The guarantee that consumers are liable for no more than $50 (and often for nothing) if a credit card is misused is essentially a form of insurance provided by issuers and merchants to credit card holders. In a competitive economy, the costs of this insurance are ultimately passed on to consumers in the form of higher prices for goods and services. Thus, the expenditures that businesses make to enhance security (and reduce the costs of fraud) will produce benefits in the form of lower prices for consumers.

Because some of the costs of fraud (around 10 percent) are borne by consumers and thus are external to the firm, the level of security might be suboptimal,[6] but only very slightly so. The level of security would be "almost optimal" since firms bear almost all of the costs directly.

B. Notification

Security and notification are two different things. While the incentives to provide security may be close to optimal, the same may not necessarily be the case for notification. The major incentive a firm or other information holding entity would have to inform consumers of the loss of data is reputational. That is, credit card issuers or others might try to use notification as a dimension of competition—for example, claiming that "we always inform you if your information is lost." If consumers value this commitment, the market would sort itself out so that those firms not promising notification would be at a competitive disadvantage.

---

5 For example, the cost of FTC advertising cases is 3-6 percent (Peltzman, 1981); the cost of Food and Drug Administration recalss is 5.6 percent (Jarrell and Peltzman, 1985); and the cost of Consumer Product Safety Commission recalls is 5.4-6.0 percent (Rubin et al., 1988).

6 That is, firms would equate private marginal costs with private marginal benefits, but social benefits of security would be higher than private benefits because firms bear only 90 percent of the costs of security braches.

There are , however, several reasons to think that this mechanism might not be adequate. Most importantly, information can be lost by many entities with no direct connection to consumers. For example ChoicePoint itself has no connection to consumers , and so would not be in a position to commit to notification. Similarly, a recent incident involved information loss by CardSystems, a previously little -known firm that processes information for credit card companies but has no connection to the card holders themselves (Dash and Zeller, 2005). Moreover, information is held and sometimes lost by firms which do not appear to be in the information business, such as retailers and universities. Such entities would not advertise information policies, and consumers would not expect them to. For example, between February and April 2005 information was lost by entities as diverse as DSW Shoe Warehouse, Boston College, Polo Ralph Lauren and Ameritrade (Wall Street Journal Online , 2005). Moreover, because of various complexities in the processing of credit card transactions , in most cases a consumer will not really know who is processing his transaction or what rules are being used (Morriss and Korosed, 2005) .[7]

In addition, characteristics of the credit card industry might adversely affect incentives for notice. Consumers are liable for at most $50 of the value of any goods or services purchased using their cards fraudulently, and in most cases even this is waived. But they must notify the card issuer of the fraud to avoid such charges. The costs are then generally borne by the merchant if a card is used fraudulently, or the issuing bank when a counterfeit card is used (Morriss and Korosec, 2005). Thus, a merchant might not have an incentive to inform a consumer of a fraudulent use because this would then cost the merchant money.

Nonetheless, it is possible that the major credit card companies (Visa, MasterCard, American Express, Discover) would require such notice for competitive reasons. These entities are sufficiently central in the contracting process that such a requirement could be enforced on all parties involved, whether the parties have a direct relationship with consumers or not.

In sum, it is unclear whether the market incentives for customer notification are adequate or not. Whether or not a regulatory notification requirement will be welfare enhancing is then an empirical question: are the expected benefits greater than the expected costs?

IV. BENEFITS OF NOTIFICATION

The benefits of a notification requirement consist of the reduction in the costs associated with identity theft. We derive a benefits estimate two ways, both of which give essentially the same result. The first estimate uses the average cost of identity theft (see Table 1) for the population as a whole as a starting point and then estimates the maximum portion of that cost that might conceivably be reduced by a notification requirement. The second estimate uses an independent estimate of the probability that

7 There are several parties involved in any transaction, including the credit card company, the bank issuing the card, and various intermediate processors, such as CardSystems.

a compromised card will be used fraudulently as the starting point. After adjusting both estimates for the effects of delay in notification, we conclude that the potential benefits of notification are on the order of $7.50 to $10 per individual whose personal information has been compromised. There is some reason to believe that even these estimates are too high.

A. Estimate 1

The expected cost per person of identity theft, based on the FTC data, is $50. This provides an upper bound for the potential benefits of any new regulatory requirement.

Javelin (2005) estimates that only 11.6 percent of the cases for which the source of the security breach is known involve an online source. Sixty-eight percent of these cases involve an offline source—for example, a lost or stolen credit card, or a relative, friend or neighbor having access to credit card bills. The remaining 20 percent presumably involved cases where it is not known whether the source was online or offline.

Notification only affects online security breaches. If we assume that all of the cases not explicitly identified to be offline are in fact online —a very conservative assumption—then only about 30 percent of the costs of identity theft could possibly be ameliorated by notification. This would reduce the maximum potential benefits to $15 per consumer.

Although we use this estimate, it is clearly still too high for several reasons. For one thing , it assumes that all breaches not explicitly identified as offline are online, when, in fact, a substantial fraction of the source-unknown thefts (perhaps the same fraction as those for which the source is known) are also offline.

In addition, notification only affects data stolen from businesses. Many online thefts do not involve businesses. Many occur, for example, when consumers are tricked into providing passwords to accounts (Pegoraro, 2005). According to one expert such theft represents "what most attackers seem to employ these days." One estimate is that about one million consumers were victims of this tactic, known as "phishing" (Pacelle, 2005).

The FTC survey indicates only 6 percent of the identity theft cases where the thief is known involve an employee of a firm .[8] In 15 percent of those cases the thief is a relative, friend or neighbor. In 14 percent, the problem is a lost or stolen card. These data suggest that only a subset of online breaches involve businesses that would be affected by a notification requirement.

---

8 The FTC study found that the thief was known in 50 percent of the cases.

B. Estimate 2

This estimate is based on an estimate attributed to Visa that 2 percent of compromised cards are used fraudulently.[9] This number also represents the probability that a compromised consumer will actually be a victim. Using the estimated consumer cost per incident of $1,000, this means that the expected cost to a person whose identity is compromised—and, therefore, the maximum benefit of notice—is $20.

The Visa 2-percent probability estimate is roughly consistent with other indirect evidence from this market. For example, some experts estimate that it does not pay for issuers to issue new cards, at a cost of between $10 and $20, for compromised accounts (Sidel and Pacelle, 2005). This cost, combined with the estimated $2,000 cost to business of an actual incident involving misuse of an existing card (see Table 1), suggests that, if it doesn't pay issuers to issue new cards, then the probability of a compromised card actually being misused must be no more than 1 percent , slightly lower than Visa's 2 -percent estimate .[10]

Evidence from underground markets that use websites to trade stolen information is also consistent with this probability estimate (Bryan-Low, 2005; Zeller, 2005). Information enabling the use of stolen cards sells for between $50 and $200 per card on such websites. Another price quoted is 5 percent of available credit. These values imply that many cards are not used, or not used intensively. If the average amount stolen from a business is $2,000 and a card sells for $200, this implies that there is only a 10-percent chance of the card actually being used; a $50 price implies a
2.5-percent chance. One gang that was recently arrested ("Shadowcrew") apparently sold two million credit card account numbers and caused over $4 million in losses to financial institutions and others. If the average loss caused was $2,000, this suggests that there were 2,000 transactions involving the two million stolen cards—a rate of 0.1 percent , significantly lower than the Visa estimate.

The news media began reporting intensely on identity theft after the ChoicePoint incident, which involved about 145,000 individuals. This was reported to the public on February 15, 2005. As of April 20, there were 750 known cases of fraud involving these individuals (Wall Street Journal Online , 2005). This is an incidence of 0.5 percent in a two-month period. If this rate continues for the entire year, then 3 percent of the compromised persons will be victimized, slightly higher than Visa's 2 -percent estimate .

In another incident, 310,000 persons were at risk from an incident involving LexisNexis on March 9. Of these, 59 cases of illegal action were known as of April 20. This represents a trivial fraction, but there may have not been enough time for victims to

---

9 This estimate is widely reported in the press (see, for example, Sidel and Pacelle, 2005). It also has been confirmed in discussions with representatives of Visa.

10 An issuer would be indifferent if the cost of the new card, say $20 was equal to the expected loss (the probability of a fraud times $2000). The probability level at which the issuer would be indifferent is 1 percent [$20 = (0.01) x ($2000)]. It would not pay for the issuer to issue a new card if the probability was less than 1 percent.

be identified in the month between the initial report of the incident (March 9) and the compilation in the Wall Street Journal (April 20).

C. Reduced Benefits Due to Delay

Providing notice to consumers takes time. A firm must first learn of the identity theft, and , while it is doing so, the thieves can be using the stolen data. Second, a firm must determine whose identities have been stolen, often by recreating the data. This is time consuming. Third, the California law and almost all other laws, whether enacted or proposed, allow the firm to delay notice if it is cooperating with a law enforcement agency. This also delays the ability of the firm to provide notice. For example, in a recent well-publicized case involving 40 million records, MasterCard observed some atypical levels of fraud in mid-April 2005, but did not provide any notice until mid-June .[11] Moreover, the FBI is still investigating the matter, so that further delay would have been possible (Dash and Zeller, 2005). Thus, in the best of circumstances, notification means that consumers might be able to respond more quickly to identity theft, not to avoid it altogether.

The FTC data provide some insight into the time profile of identity theft losses. For those consumers who discovered identity theft within five months, 67 percent had no out of pocket expenses. For those who did not discover the theft for six months or more, only 40 percent had no out of pocket costs. For those who discovered the theft within one month, 76 percent were able to resolve their problems in less than 10 hours, while for those who discovered the theft after more than six months only 20 percent were able to accomplish this in less than 10 hours. These data are difficult to extrapolate , but they suggest that normal notification delays can have a significant effect on losses, if active identity thieves are involved. We assume this factor reduces the benefits of notice by 50 percent. This reduces the benefits to about $7.50 to $10.

D. Consumer Response

Even when consumers receive notice of a security breach, many of them do nothing about it. For most people, this is probably the best response, because most compromised data are not misused and “doing something about it” is far from costless. The FTC survey indicates that even among those who have been victims of identity theft, 55 percent indicate that they are “not very” or “not at all” concerned that they will be victimized again. Thirty-eight percent of victims reported to no one, including even the credit grantor or place of misuse. The FTC indicates that only 26 percent of actual victims reported to the police and only 22 percent of victims reported to credit bureaus; of these, 62 percent asked for a “fraud alert.” In other words, only 14 percent of actual victims asked for a fraud alert. Thus, if only a small percentage of actual victims make use of alerts, it is unlikely that many persons who only were notified of a breach will do so, because the probability of actual ID theft is still very small.

[11] It is not clear that the notice provided by MasterCard was consistent with the requirements of the various state laws.

As indicated above, the evidence suggests that only about 2 percent of those who are exposed are actually victimized. In addition, for most forms of victimization, the costs are minimal; credit cards guarantee that consumers pay a maximum of $50 of any loss. Finally, in many cases, the costs (in inconvenience) of taking action may be as great or greater than the costs of being victimized—and the costs of taking action are certain, while the costs of victimization are only probabilistic and are only incurred in the unlikely event that one is actually a victim.

The fact that most consumers do not take any action when notified further reduces the benefits of notice. Nonetheless, we do not adjust for this factor since there is no current way to measure the probability that a compromised individual will actually take any action. Thus, the benefit estimate of $7 .50 to $10 may be biased upwards. Any actual benefit will likely be less than that amount.

V. COSTS OF NOTIFICATION

There are three categories of potential costs associated with a notification requirement: the direct notification costs ; the costs of actions taken by consumers as a result of notification; and the costs in terms of a diminished flow of information resulting from actions that firms might take in response to a publicized security breach.

A. Direct Notification Costs

The California statute requires written or electronic notice, but it allows "substitute notice" if the "cost of providing notice would exceed two hundred fifty thousand dollars or the affected class or subject persons to be notified exceeds 500,000." "Substitute notice" includes emails, posting on a website, and notification of major statewide media. Other state bills, proposed and enacted , seem to have adopted a similar approach. This would place the maximum cost of notification at $250,000.[12] Given that the upper bound estimate of the benefit of notice seems to be no more than $10 per person (as discussed above), any breach involving more than 25 ,000 victims might justify the cost of notice.[13] The cost of writing a letter has been estimated at $2 per person (Sidel and Pacell, 2005), which would imply that notice might barely be worthwhile if this was the only cost . However, there are additional costs that are more important .

B. Costs of Actions Taken by Consumers

Costs to consumers as a result of actions they take may be more significant than the direct costs to firms of providing notice. The FTC (FTC, n.d.) and others recommend the following actions for those who are or suspect they are the victims of identity theft: Place a fraud alert on your accounts and close the accounts "that you know, or believe " have been tampered with fraudulently. A fraud alert means that a

[12] As shown below, the cost might be much greater because of the lack of coordination between states.
[13] This discussion does not take into account the fact that there is likely to be some variation in the effectiveness—and therefore the expected benefits—associated with the different methods of notification. Otherwise, there would be no point in not permitting the least-expensive methods to begin with.

business must verify the consumer's identity before issuing credit, generally by contacting the consumer directly before issuing credit. The FTC indicates that "[t]his may cause some delays if you're trying to obtain credit." In many circumstances, the agency also recommends closing accounts , which may be even more costly, particularly if consumers have set up accounts to automatically pay recurring bills.

All these costs are likely to be significantly greater than the expected costs of compromised individuals actually being victimized. Recall that we estimated these costs to be about $20. This explains why it is perfectly rational for most consumers to do nothing, even when notified that their data have been compromised.

Additionally, consumers can impose costs on firms. A consumer notified about some threat may request a new card. The cost of issuing a new card is estimated at between $10 and $20, which is about equal to the expected cost (to the consumer) of actually being a victim.

There is an even more significant potential cost, which is difficult to quantify. As consumers start to receive more notices, they may become increasingly afraid to do business online (Fountain, 2005). This would be a costly reaction, because, as the Javelin Report shows, online commerce is safer than traditional offline commerce. For example (p. 7): "the current data on the source of access clearly evidences that consumers are most at risk when using traditional methods." A second finding (p. 10) is that "[t]he single most effective approach to protect against both external and domestic identity theft is to turn off all paper bills and statements." The Javelin Report also indicates (p. 4) that the mean time for fraud detection for paper statement review is 114 days, with a mean cost of $4,543; the comparable numbers for electronic accounts are 18 days and $551. It is quite plausible that a continual stream of warnings could lead consumers to decide that online commerce is riskier than traditional offline paper commerce and, consequently, shift away from the online mode. This would have the effect of increasing the identity-theft risks to which they are exposed.

C. Information Costs

As discussed above, if a firm provides notice of loss of data under its control, it will suffer a loss of reputation and share value . From society's point of view, however, the threat of a loss of reputation may be a good thing , stimulating firms to provide better security for their data. Thus, the private cost to the firm may be socially beneficial.

Firms may, however, overreact in an effort to minimize the costs associated with loss of reputation. We know that the information provided by firms in the information market is of great value to consumers and the economy (Rubin and Lenard, 2002). Any reaction that reduces the value of this information can easily outweigh any benefits of notice. For example, as a result of a reaction to the loss of information on 300,000 individuals, LexisNexis began restricting access to Social Security and drivers' license numbers to a limited class of users (New York Times, 2005). ChoicePoint has also begun restricting use and provision of its information in many ways (Solove and

Hoofnagle, 2005). One fallout from these policies is that it will be more difficult for new firms to enter some markets, because it will be more difficult for them to obtain the necessary customer data. It is likely that the net effect of these and similar policies will be to reduce consumer welfare.

VI. ARE THE BENEFITS OF NOTIFICATION GREATER THAN THE COSTS ?

The expected benefits to consumers of mandatory notification are only about $7.50 to $10 per individual whose personal data has been compromised due to a security breach. This is obviously an extremely small number.

There are several reasons that the expected benefits are so small: First, most cases of identity theft involve offline security breaches, which are not affected by notification. Second, the probability of an individual compromised by an online security breach becoming an identity theft victim is extremely small. Third, most of those victims don't really have their identity stolen. Instead, the fraud consists of charging items to the victims' accounts—charges for which the account holders have very limited liability. Finally, even a well-designed notification program is likely only to eliminate a small fraction of the expected costs—we estimate about 10 to 20 percent.

Given these very small expected benefits, it is difficult for a notification mandate to pass a benefit-cost test. While the direct costs to notifying firms may not be large, the indirect costs both to consumers and to sectors of the economy that depend on the free flow of information are likely to be substantial, primarily because of the likelihood that both consumers and firms suffering a security breach will overreact to notification. Of particular concern is the fact that consumers would increase their risk exposure if they shifted from online to paper -based transactions as a result of the publicity associated with multiple notifications.

Finally, this all should be put in the context of the trend data, which indicate that the true risk of identity theft and related frauds is not increasing and may actually be decreasing over time. Thus, the market incentives seem to be alleviating the problem and it is likely that consumers' perceptions of the risks—which perhaps currently are exaggerated—will adjust accordingly.

VII. OPTIMAL SCOPE OF NOTICE

The discussion above suggests that any notification requirement is dubious on benefit-cost grounds. Thus, any new statute that is passed should be carefully targeted to individuals most at risk.

There are several dimensions on which mandated disclosures could be targeted. One is encryption. The California law deals only with unencrypted data, and this is a useful limitation. Since only a small percentage of compromised records are actually misused, it is very unlikely that encrypted records are among them.

A second issue concerns the population to be notified (Pacelle and Conkey, 2005). In situations where the firm has good reason to believe that only a fraction of the potentially compromised consumers are at risk, the notice should be tailored to those consumers. In addition to the direct expense, an overly broad notification requirement might cause consumers to become inured to receiving such notices or to withdraw needlessly from various forms of commerce due to excessive fear of identity theft (Fountain, 2005.) This is especially dangerous since, as mentioned above, online commerce is actually safer than offline commerce.

VIII. THE ISSUE OF PREEMPTION

Thus far, security breach legislation has been introduced in at least 35 states and adopted in at least 13 states : Arkansas, California, Connecticut, Florida, Georgia, Illinois, Indiana, Maine, Minnesota, Montana, North Dakota, Texas and Washington. Bills are now sitting on the governor's desk in Nevada and Tennessee. The question is whether it would be better to allow each state to approach this issue as it sees fit or to have a federal law that preempts state laws and subjects the whole country to the same set of rules.

A. Benefits of Federalism

As a general matter, there are two major benefits to a federalist approach. The preferences of individuals may not be the same everywhere and it is better if states are able to adopt rules tailored to the preferences of citizens. In addition, a federalist approach makes it possible to experiment with different rules at the state level (the states can be laboratories) and this can reduce the risks associated with adopting a single set of rules at the federal level that may be flawed in ways that we don't foresee.

It is questionable, however, whether true federalism is possible for firms operating in a market that is (at a minimum) national in scope. For these companies, information breaches don't just affect citizens in one state. When a breach occurs, virtually any firm that operates in a number of states will apply the same notification policy to everyone affected.

The California law went into effect in 2003, but the major event drawing attention to the issue was the ChoicePoint incident in early 2005. Initially ChoicePoint planned to disclose the breach only to California residents, as required by law. However, once the breach was publicized, pressure quickly mounted to make the same disclosure to everyone who was affected. Since then, most (if not all) firms suffering breaches have followed the same policy and disclosed to everyone. If this is the general practice, then it appears that the most stringent state law or set of provisions taken from various state laws (in the sense of requiring disclosure to the largest number of people in the largest set of circumstances) will govern all states. We would not have the benefits of a federalist approach even if the federal government does not formally preempt state laws. Rather , there will be implicit "preemption" by the most regulatory state or states .

This also applies to the levels of data security that firms maintain, which are closely related to disclosure requirements and are often part of data security legislation. But levels of security are determined in a national market and firms such as ChoicePoint and CardSystems are not going to maintain different levels of security for residents of California than for residents of New York. In a truly federal system citizens with greater preferences for security would pay for this security. But in this market, where firms maintain the same level of security for all individuals, individuals in states with a greater preference for security can impose the costs of these preferences on the entire country.

Federalism would seem to be possible only for regulations that apply to the information practices of businesses small enough to operate within one state. But the publicized security breaches have been for firms that operate nationally and internationally. Adopting a federalist approach to the regulation of these firms does not seem feasible.

B. Benefits of Preemption

1. Inconsistencies in State Statutes

The laws already in place at the state level have major inconsistencies with respect to critical provisions : the definition of personal data; when notice is required; and who must be notified:[14]

Definition of personal data . In California "personal data" include computerized data containing name; social security number; drivers' license number; and account number with access code. Other state statutes include these data in their definitions , but add additional items. In Texas, personal data include unique biometric data. In Arkansas, personal data include some medical data. In Ohio, all personal data, not merely computerized data, are covered by the law. In Montana, all data are covered and data include passport number and insurance policy number. In Georgia, only data held by information brokers are covered (perhaps in response to ChoicePoint which is an information broker and a Georgia firm). Breaches involving encrypted data are exempt from notification requirements in California, but other states differ. In New York notice is required if data are encrypted but an encryption key is also acquired by the thieves. If we assume that the most restrictive laws will govern, then notice will be required for all data (computerized or not) including biometric data and passport and insurance policy number and including encrypted data if the key is also stolen. In other words, the actual policy will be a mixture of the most restrictive aspects of each state policy, so that it will be more restrictive than any one state.

[14] Information on a sate by state basis is available at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm. This site has links to bills and was used in examining the laws discussed in this section. We do not provide a comprehensive analysis of the various statutes; the only point we are making is that even a casual reading indicates that the laws differ in economically significant ways which will greatly increase costs of compliance.

When notification is required. Most states allow for a delay in notice for the purposes of cooperating with a law enforcement agency. However, the Illinois law does not allow such a delay. [15] Most states allow delay while the firm determines the scope of the breach and makes an effort to restore the security of the data; California does not. [16] This means that in California notice must occur while firms are still determining what has been stolen and while security flaws have not been fixed, which could trigger more invasions. Connecticut allows an exemption if the business, after consultation with federal, state and local agencies, determines the breach will not likely result in harm, and in Washington a firm need not disclose a technical breach that does not seem reasonably likely to subject customers to risk of criminal activity. While these two exemptions are reasonable, the fact that only two states have them means that they will not provide any benefits in practice.

Type of notification required. In California, consumers must be notified about a breach. In New York, notice must include a description of the categories of data involved. In many states, in addition to notifying consumers, the credit bureaus must also be notified, but the rules triggering this notice vary. In Indiana and Nevada credit bureaus must be notified if more than 1,000 records are compromised; in New York, 5,000 records; and in Texas and Georgia, 10,000 records are needed to trigger this notice. The result will be that consumers in all states will be notified and will be given a description of all data, and credit bureaus will also be notified if more than 1000 individuals are involved.

Moreover, this set of requirements is based on thirteen states. As additional states pass laws, requirements will shift, and as states modify their laws, they will shift again. Thus, firms will be forced to monitor fifty state legislatures to determine what set of requirements is most restrictive at any time.

2. The Effect of the Inconsistencies

We argued above that a federalist approach is not really feasible in this market—that for companies operating at the national level the most stringent set of rules will be binding. Thus, for the most part, we do not envision a situation in which companies will be faced with the prospect of complying with 50 different sets of rules. Nevertheless, companies potentially will be faced with the prospect of familiarizing themselves with all those rules, to make sure they are in compliance. The costs associated with this, which probably do not vary much with firm size, would constitute a particular burden for smaller firms.

Notwithstanding the tendency to gravitate to the most stringent set of requirements, there are some inconsistencies that could be costly. For example, all state statutes have a provision that "alternative notice" (emails, posting on a website, notification of major media) is allowed if individual notice is above certain trigger

[15] This may be an oversight, but it is not mentioned in the Illinois statute.

[16] This may be something learned after the California law was adopted, and may be a benefit of Federalism.

levels—generally 500,000 consumers or a cost of $250,000. But there seems to be no coordination of this requirement across states. Thus, if 450,000 consumers in each state are involved and the cost in each state of individual notice is $200,000 a firm might end up being forced to notify 22 .5 million consumers at a cost of $10 million.

These multiple state rules, even if the same, may also lead to confusion among victims. Take, for example, the case where two states both allow alternate notice if more than 500,000 consumers are involved, as the California law does. In State A, 200,000 consumers are involved, so written notices are sent out; in State B, 600,000 consumers are involved, so a notice is posted on the website of the business, an acceptable form of "alternate" notice. Faced with these notices, a consumer in State A could easily assume that two separate breaches have occurred since he will receive a written notice and also see the website warning.

In one draft federal bill,[17] alternate notice is allowed if more than 500,000 consumers are involved or if the cost of direct notices is more than $500,000. This provision itself could save firms (and thus consumers) millions of dollars and lead to reduced confusion.

C. The Benefits of Federalism vs. the Benefits of Preemption

As we discussed above, a true federalist approach does not really seem to be feasible in this market, which is national in scope. The proliferation in state laws will yield some inconsistencies that will impose costs on firms and consumers. But as much as possible, firms will react by complying with the most stringent set of regulations. It is better to have this policy set at the national level, by lawmakers who presumably are representative of the nation as a whole, rather than have one state or one set of states "preempt" policies for the rest of the country.

IX. CONCLUSION

A series of highly publicized data security breaches have created the perception that identity theft and related frauds are a large and growing problem , in need of a new regulatory solution. But, this perception is not borne out by the actual data , which indicate that, depending on the time period and measure used, identity theft has been either constant or diminishing over time. Thus, calls for new regulation should be treated with some skepticism.

It should not be surprising that the market seems to be working fairly well to restrain identity theft. Firms in the credit industry bear most of its costs and have a strong incentive to keep those costs under control.

The major finding of this study is that the costs of a notification requirement are likely to be substantially higher than the benefits. Even for consumers whose data has been compromised, the probability of being a victim of fraud is so low—only 2 percent—

[17] Notification of Risk to Personal Data Act, S. 751.

that little action is justified. Overall, we estimate that the expected benefits of mandatory notification are very small—less than $10 per compromised individual.

The major regulatory costs to be concerned about are not the direct costs of notification. Rather, they are the costs incurred when consumers and firms overreact and take actions that are harmful to themselves and to the free flow of information. Consumers, for example, may be induced to place fraud alerts on their accounts or close them entirely, actions that are likely to be far more costly than being an identity theft victim. They may also be induced to shift their credit transactions offline, which the data show would actually increase their exposure to identity theft.

Firms in the information business may start limiting access to their information in an effort to protect their reputations. But this information is valuable to consumers and the economy and restricting it can have significant costs.

Because a notification mandate is dubious on benefit-cost grounds, it should be carefully targeted to those individuals most at risk in order to increase its potential benefits. Federal preemption of inconsistent state requirements will lower its costs. While these measures can help the benefit-cost balance, it is doubtful that they will be sufficient to bring that balance to the point where the benefits of notification mandate will be sufficient to offset the costs.

REFERENCES:

Bank, David and Don Clark (2005), Visa sets antifraud system upgrade, Wall Street Journal, June 13, p. B4.

Bryan-Low, Cassell (2005), Identity thieves organize, Wall Street Journal, April 7, p. B1.

Bureau of Labor Statistics (2005), Real earnings in May 2005, press release, June 15.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou (2003), The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, 11, 431-448.

Dash, Eric and Tom Zeller (2005), MasterCard says 40 million files are put at risk," New York Times, June 18.

Federal Trade Commission (n.d.), Take charge: Fighting back against identity theft, available on the FTC website.

Federal Trade Commission (2005), Identity theft survey report, Synovate, September, available on the FTC website.

Fountain, Henry (2005), Worry, but don't stress out," New York Times, June 26, Section 4, p. 1.

Garg, Ashish, Jeffrey Curtis, and Hilary Halper (2003), Quantifying the financial impact of IT security breaches," Information Management & Computer Security, 11/2, 74-83.

Jarrell, G. and Peltzman, S, (1985), The impact of product recalls on the wealth of sellers, Journal of Political Economy, 93, 512-536.

Javelin Strategy & Research (2005), 2005 identity fraud survey report (abbreviated summary available online).

Morriss, Andrew P. and Jason Korosec (2005), Private dispute resolution in the card context: structure, reputation, and incentives," Case Research Paper Series in Legal Studies, Working Paper 05-12, June, available at http://ssrn.com/abstract=735283.

New York Times (2005), Company news: LexisNexis restricts access to personal data," March 19, nytimes.com.

Nilson Report (2005), Credit card fraud in the U.S., March, partially available online.

Pacelle, Mitchell (2005), How MasterCard fights against identity thieves, Wall Street Journal, May 9, p. B1.

Pacelle, Mitchell and Christopher Conkey (2005), Card Industry Fights Breach Bills, Wall Street Journal, June 23, p. C1.

Peltzman, S. (1981), The effects of FTC advertising regulation, Journal of Law and Economics, 24, 403-448.

Pegoro, Rob (2005), Voluntary disclosure is the threat to password security," Washington Post, June 12, p. F 7.

Rubin, Paul H. and Thomas M. Lenard (2002), Privacy and the commercial use of private information, Boston, Kluwer Academic Publishers and the Progress and Freedom Foundation.

Rubin, P.H., R.D. Murphy and G. Jarrell (1988), Risky products, risky stocks, Regulation, 35 -39.

Sidel, Robin and Mitchell Pacelle (2005), Credit-Card breach tests banking industry's defenses," Wall Street Journal, June 21, p. C1.

Solove, Daniel J. and Chris Jay Hoofnagle (2005), A model regime of privacy protection: Version 2.0, available from SSRN.com.

Wall Street Journal Online (2005), Without a trace: A Wall Street Journal online news roundup, April 20.

Zeller, Tom (2005), Black market in stolen credit card data thrives on Internet," New York Times, June 21.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
voice: 202/289-8928 ■ fax: 202/289-6079 ■ e-mail: mail@pff.org ■ web: www.pff.org