Does the rush to pass state-level data security regulations benefit consumers?

Much Ado About Notification

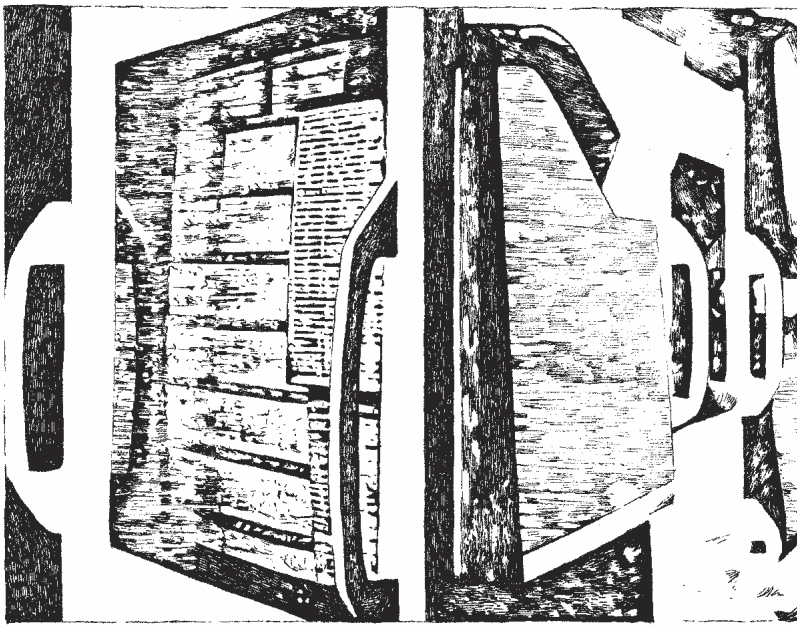
By Thomas M. Lenard, *Progress & Freedom Foundation*
and Paul H. Rubin, *Emory University*

CONGRESS AND THE STATES ARE MOVING rapidly to enact new legislation in the wake of a series of high-profile data security breaches at both private and public institutions. A major objective of all the pending bills is to require that consumers be notified when a breach occurs that might compromise their confidential information.

A notification requirement has been in effect since 2003 in California, which (not surprisingly) was the first state to enact such a statute. Indeed, the California 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, at least 13 states have security breach legislation in place.

Press accounts and statements from various experts give the impression that identity theft and related frauds are increasing at a rapid rate. For example, the preamble to the California statute states, "Identity 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 two surveys by research firms, the first one commissioned by the Federal Trade Commission and carried out by Synovate in 2003, and a subsequent update of the FTC study undertaken in 2004 by Javelin. Virtually all the results of the two studies, including the incidence of identity theft and the costs to victims, are about the same, indicating that fears of identity theft being a rapidly growing problem are exaggerated. Indeed, the actual incidence of identity theft of all forms decreased from 4.6 percent of the adult population to 4.25 percent, although this difference was not statistically significant.

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 the costs have been decreasing over time. Estimates by *Nilson* (a trade publication for the credit card industry) show the total costs of credit card fraud to issuers decreased from $0.157 to $0.047 per $100 in credit card sales from 1992 to 2004. This is not surprising because, despite the press accounts, credit



Thomas M. Lenard is vice president for research at the Progress & Freedom Foundation. He may be contacted by e-mail at tlenard@pff.org.

Paul H. Rubin is the Samuel Candler Dobbs Professor of Economics and Law at Emory University and senior fellow at the Progress & Freedom Foundation. He may be contacted by e-mail at prubin@emory.edu.

card firms are continually updating and improving security. The *Nilson* report also indicates that fraudulent charges as a percentage of credit card use are lower in the United States than in other countries.

THE COSTS OF SECURITY BREACHES

The FTC estimates that 10 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 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—constitutes two thirds of the total number of incidents. The remaining third consists of opening 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 article, 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.

The per-victim cost of new-account fraud is $1,180 and 60 hours of time. Using $15 per hour—the Bureau of Labor Statistics average wage rate—as an estimate of the value of time, 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. As 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.

TABLE 1

Costs of Identity Theft

2003

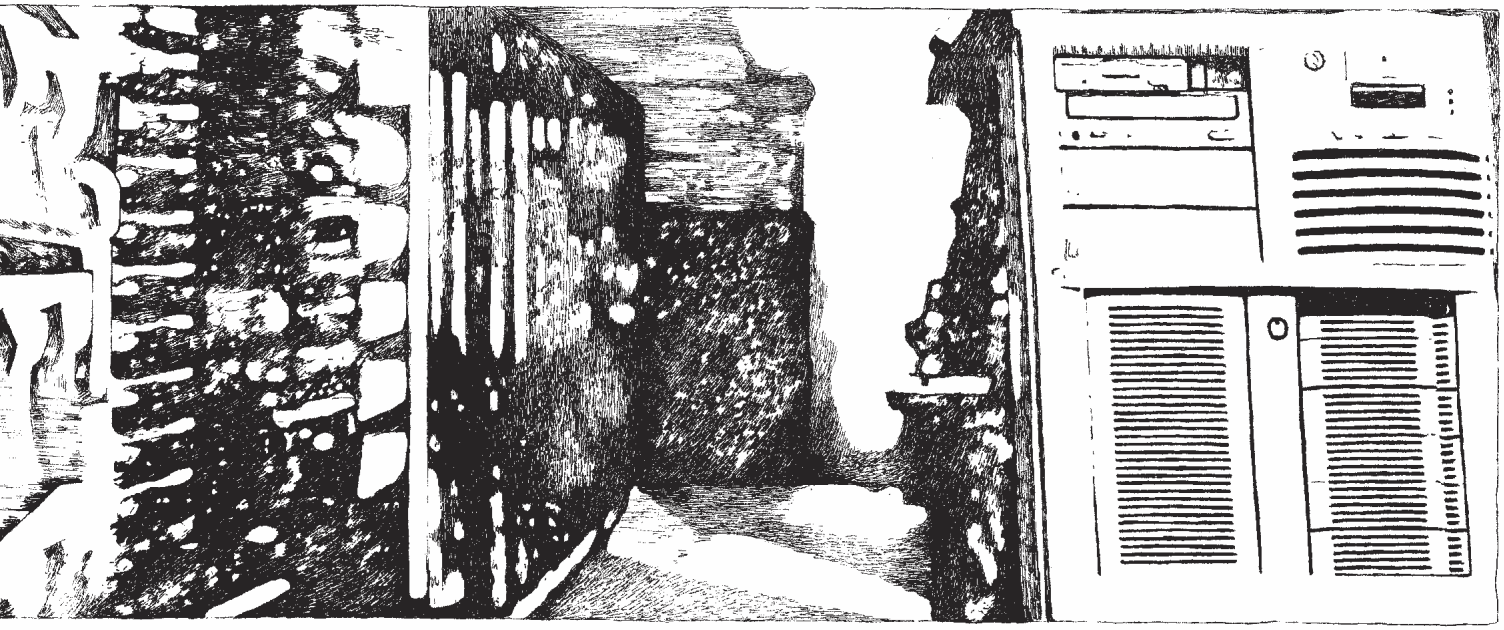
	New-Account Fraud	Existing-Account Fraud	Total
Incidence	1.5%	3.1%	4.6%
Weight	0.326	0.674	1.00
Cost to businesses	$10,200	$2,100	$4,800*
Cost to individuals	$1,180	$160	$500*
Time spent by individuals	60 hrs.	15 hrs.	30 hrs.*
Cost of time @ $15 per hour	$900	$225	$450*
Total cost to individuals	$2,080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

* Weighted averages of new and existing account fraud (totals are rounded).
SOURCE: Computed from "Identity Theft Survey Report," prepared by Synovate and published by the Federal Trade Commission, September 2003. Available on the FTC Web site.

MARKET RESPONSES

Possible responses to the risk of this type of fraud can be grouped into two categories: *ex ante* and *ex post*. The most prominent *ex ante* approach is improved security. One of the more common state regulations concerning data security is an *ex post* approach: mandatory notification of the victim in the event of a security breach.

IMPROVED 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—credit card companies, banks, merchants and others—should have a strong incentive to invest in data security.



MORGAN BALLARD

The costs to firms are reflected in the large stock market losses they suffer when victimized by security breaches. In a 2003 *Information Management & Computer Security* article, Ashish Garg, Jeffrey Curtis, and Hilary Halper 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. That cost is quite large—three to five times the amount found in similar studies for other classes of events. A *Journal of Computer Security* article that same year by Katherine Campbell, Lawrence Gordon, Martin Loeb, and Lei Zhou found that breaches associated with violations "such as customer databases" 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 loss might create an incentive for firms to keep information regarding breaches from becoming public, although there may be policies from other agencies, such as the Securities and Exchange Commission, that require notification. If this is not the case, a policy requiring public notice of breach but not requiring notification to each individual victim would be much cheaper than the policy discussed here. (Of course, this would apply only to publicly traded firms. Universities, medical facilities, and government agencies, which account for a large fraction of the total number of breach victims, are not affected by this issue.)

The incentive to reduce costs associated with identity theft 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. 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) produce benefits in the form of lower prices for consumers.

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

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. Businesses 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 valued this commitment, the market would sort itself out so that firms not promising notification would be at a competitive disadvantage.

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. Nonetheless, it is possible that the major credit card companies would require such notice for competitive reasons. Those 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.

Moreover, information is held and sometimes lost by firms that 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. 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.

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 that is waived.

Firms have a very strong incentive to avoid data security breaches because the market penalizes them severely if breaches occur.

But to avoid such charges, they must notify the card issuer of the fraud. The costs are then generally borne by the merchant or the issuing bank. Thus, a merchant might not have an incentive to inform a consumer of a fraudulent use because notification would cost the merchant money.

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?

BENEFITS OF NOTIFICATION

The benefits of a notification requirement consist of the reduction in the costs associated with identity theft. After adjusting the estimate for the effects of delay in notification, we conclude that the potential benefits of notification are on the order of no more than $10 per individual whose personal information has been compromised. There is some reason to believe that even those estimates are too high.

Our estimate is based on a determination attributed to Visa that two percent of compromised cards are used fraudulently. 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 two-percent estimate applies only to thefts involving credit card numbers. The most common type of information disclosed in security breaches appears to be Social Security numbers. Since these are more difficult to use than credit card numbers, it is likely that rate of misuse is no higher than two percent, and may be much lower.

The Visa probability estimate is roughly consistent with other indirect evidence from this market. For example, some experts believe that it does not pay for issuers to issue new cards with different account numbers, at a cost of between $10 and $20, for compromised accounts. This cost, combined with the estimated $2,000 cost to business of an actual incident involving misuse of an existing card, suggests that if it does not pay issuers to issue new cards, then the probability of a compromised card actually being misused must be no more than one percent, lower than Visa's estimate.

Evidence from underground markets that use Web sites to trade stolen information is also consistent with this probability estimate. The "Shadowcrew" gang that was recently arrested 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.

REDUCED BENEFITS Providing notice to consumers takes time. A firm must first learn of the identity theft and then determine whose identities have been stolen, often by recreating the data. This gives the thieves time to take advantage of the stolen data.

The California notification law and almost all other laws, whether enacted or proposed, allow the firm to further delay notice if it is cooperating with a law enforcement agency. 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. The FBI was still investigating the matter when MasterCard provided notice, so further delay would have been possible.

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. We assume this factor reduces the benefits of notice by 50 percent. This reduces the benefits to about $10.

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 say 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. 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 identity theft is still very small. 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 actually is 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 because there is no current way to measure the probability that a compromised individual will actually take any action. Thus, the benefit estimate of $10 may be biased upwards. Any actual benefit will likely be less than that amount.

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.

DIRECT COSTS The California statute requires written or electronic notice, but it allows "substitute notice" if the cost of providing notice would exceed $250,000 or "the affected class or subject persons to be notified exceeds 500,000." "Substitute notice" includes e-mails, posting on a Web site, 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. Given that

the upper bound estimate of the benefit of notice seems to be no more than $10 per person, any breach involving more than 25,000 victims might justify the cost of notice. However, there are additional costs that are more important.

COSTS OF CONSUMERS' ACTIONS 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 and others recommend the following 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 business must verify the consumer's identity before issuing credit, generally by contacting the consumer directly. The FTC notes, "This 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 pay recurring bills automatically. Moreover, if notice leads consumers to spend several hours of time (valued at an average of $15 per hour) monitoring their accounts, this can actually outweigh any benefits.

All those costs are likely to be significantly greater than the expected costs of compromised individuals actually being victimized. 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. This would be a costly reaction because, as the Javelin report shows, online commerce is safer than traditional offline commerce. For example, "the current data on the source of access clearly evidences that consumers are most at risk when using traditional methods." A second finding is, "The 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 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. Overall, over 70 percent of all identity theft occurs from offline activities. 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. There is some evidence that this is occurring. This would have the effect of increasing the identity-theft risks to which they are exposed.

INFORMATION COSTS 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, 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. 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. ChoicePoint has also begun restricting use and provision of its information in many ways. One result 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.

ARE THE BENEFITS GREATER THAN THE COSTS?

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

Given the 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 will increase their risk exposure if they shift from online to paper-based transactions as a result of the publicity associated with multiple notifications.

Because any notification requirement is dubious on benefit-cost grounds, 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. Because only a small percentage of compromised records are actually misused, it is very unlikely that hard-to-decipher encrypted records are among them.

A second issue concerns the population to be notified. 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 because of excessive fear of identity theft. This is especially dangerous because online commerce is actually safer than offline commerce.

FEDERAL PREEMPTION

Thus far, security breach legislation has been introduced in at least 35 states and adopted in at least 13 states. 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.

FEDERALISM'S BENEFITS As a general matter, there are two major benefits to a federalist approach. The preferences of individuals may not be the same everywhere and states are in a better position to tailor rules 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 do not 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 those companies, information breaches do not 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, and other firms seem to 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 will 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 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 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 their preferences on the entire country.

It might appear that because firms like ChoicePoint are in the business of maintaining data on individual consumers, requiring those firms to keep track of requirements for consumers in different states would not be difficult. But many firms that maintain data do not have the size or resources of a firm like ChoicePoint. A requirement to monitor 50 sets of state regulations would impose a burden on small firms and on new entrants, thus skewing the market toward large firms.

INCONSISTENCIES 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.

It is questionable whether federalism is possible for firms operating in a market that is (at minimum) national in scope.

In all state regulations, the definition of personal data always includes computerized data containing name, Social Security number, drivers' license number, and account number with access code. Some state statutes add additional items including unique biometric data, some medical data, all personal data (not merely computerized data), passport number, and insurance policy number. Breaches involving encrypted data are exempt from notification requirements in some states but not others. If the most restrictive laws govern, then notice will be required for all data (computerized or not), including biometric data, passport and insurance policy numbers, and encrypted data. 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 even the most restrictive state.

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. 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. This means that in California, notice must occur while firms are still determining what has been stolen and while security flaws are still being fixed—which could trigger more invasions. Some states allow exemptions when breach is not likely to result in harm, but those exemptions will not provide any benefits in practice because other states do not allow them.

In California, consumers must be notified about a breach. In other states, 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, ranging from 1,000 to 10,000 compromised consumers. The result of those differences is 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 1,000 individuals are involved.

Moreover, this set of requirements is based on 13 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 50 state legislatures to determine what set of requirements is most restrictive at any time.

EFFECT OF 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, will 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" (e.g., e-mails, posting on a Web site, notification of major media) is allowed if individual notice is above certain trigger 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.

In one draft federal bill, 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.

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.

CONCLUSION

A series of highly publicized data security breaches has created the perception that identity theft and related frauds are a large and growing problem, in need of a new regulatory solution. But the data are not consistent with that perception. The data indicate that 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 the costs of fraud 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 have been compromised, the probability of being a victim of fraud is so low—only 2 percent—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 those 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 a notification mandate will be sufficient to offset the costs. R

READINGS

- "An Economic Analysis of Notification Requirements for Data Security Breaches," by Thomas M. Lenard and Paul H. Rubin. Progress & Freedom Foundation, 2005.
- "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," by Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. *Journal of Computer Security,* Vol. 11 (2003).
- *Privacy and the Commercial Use of Private Information,* by Paul H. Rubin and Thomas M. Lenard. Boston, Mass.: Kluwer Academic Publishers, 2002.
- "Private Dispute Resolution in the Card Context: Structure, Reputation, and Incentives," by Andrew P. Morriss and Jason Korosec. Case Research Paper Series in Legal Studies, Working Paper 05-12, June 2005.
- "Quantifying the Financial Impact of IT Security Breaches," by Ashish Garg, Jeffrey Curtis, and Hilary Halper. *Information Management and Computer Security,* 2003.