TOWARDS A RATIONAL PERSONAL DATA BREACH NOTIFICATION REGIME

BY
MICHAEL TURNER

Information Policy Institute | JUNE 2006

Table of Contents

EXECUTIVE SUMMARY

Identity theft is a significant problem in need of federal legislation. Any standard for breach notification must be uniform and therefore national. Allowing states to regulate the issue entails potential problems. We come to this conclusion on the basis of the following observations:

1) In the event that breach notification triggers are set at the state level, national firms are likely to adhere to the most stringent standard. If possible, because of the efficiencies of complying with one regulatory standard as opposed to many. Where it is not, firms will apply patchwork responses, many of which will involve confusion.

2) The trigger mechanism for breach notification must be appropriately calibrated: a standard that sets the threshold too "low" will cause some consumers to ignore breach notices.

3) A federal standard will protect consumers in states where legislatures are slow to act or ignore the problem of data breaches altogether.

In considering the need for breach notification, it's important to keep in mind that, while the scale and scope of identity theft crimes are significant, the figures are comparable to statistics for other property crimes. Perhaps more telling when considering government intervention is the fact that the costs, incidence, and time necessary to address identity crime incidences have all declined in recent years.

Presumably this is due, at least in part, to industry efforts to curb financial fraud and ID theft through greater investment in fraud detection and information security.

1) The costs of credit card fraud declined by 10% in 2004 from its 2003 level. [1]

2) Rates of identity crime (that is, incident per 100 people) fell between 2003 and 2004 for both existing credit card fraud and new account fraud, from 2.6% (2003) to 2.28% (2004) and from 1% (2003) to 0.83% (2004), respectively.

3) Between 2003 and 2004, the mean resolution time for an incidence of identity theft declined by 15%.

4) Industry efforts to curb financial fraud and ID theft through greater investment in fraud detection and information security has lead to significant reductions. Credit card fraud, as a share of credit card sales, has fallen from 0.18% in 1992 to 0.06% in 2004.

---

1 Thomas Lenard and Paul Rubin, "*An Economic Analysis of Notification requirements for Data Security Breaches*", Progress and Freedom Foundation. July 2005.

UNDERSTANDING DEFINITIONS OF IDENTITY THEFT

Identity theft and identity fraud have emerged as serious crimes for consumers, citizens and business. There are no comprehensive statistics on identity theft over time, but many indicators suggest that it has grown in the last decade (though see below for changes in trends).[2] Given the peculiar nature of this type of theft—namely, that it can be perpetrated by accessing information stored in places uncontrolled by the victim and in places of which the victim is often unaware—legislators have passed or are considering passing laws which require that the consumer be notified in the event of a data breach.

The category of identity crimes consists of two distinct types of thefts, "account takeover" and "true name fraud". "Account takeover" is the more common form and involves the unauthorized use of financial account information to make fraudulent purchases or steal money from the victim. In practice, it encompasses events such as the theft of a credit card from a wallet and the unauthorized use of a credit card by an associate, friend, or family member.

"True name fraud" is the more sensational and costly form of identity crime and involves the theft of information about an individual that allows the criminal to open new accounts in the name of the victim.[3]

In the most common types of identity fraud, credit card fraud, victims are typically liable for only $50 of the losses, a limit that is often waived by lenders.

Typically, the two are lumped together as ID theft, in spite of the differences between them. The two are linked in the minds of ordinary people, the media, and the law.[4] Unauthorized access of credit card information from a database conjures images of criminals with complete credit and financial identity information.

---

2 A few indicators are available. One CRA reported an increase in fraud alters in 2000 over 1999 -from approximately 65,600 in 1999 to 89,000 in 2000. Another reported an increase from 19,347 during July 1999 through June 2000 to 29,593 during July 2000 through June 2001). The FTC's Identity Theft Data Clearinghouse received an average of 445 calls per week when it opened in November 1999. By March 2001, it was receiving 2,000 per week, and 3,000 answered calls per week the following December. The SSA/IOG reported 11,000 cases of alleged SSN misuse in fiscal year 1998; in fiscal year 2001, it received 65,000 reports. See Richard Stana, "*Identity Theft: Available Data Indicate Growth in Prevalence and Costs.*" GAO. Before the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, US Senate. (Washington, DC: General Accounting Office, February 14, 2001) GAO-02-424T. www.gao.gov/new.items/d02424t.pdf. Though the trend appears to have changed, see below.

3 It should be noted that Congress has defined ID theft so that it encompasses ID fraud. Discussions of the issue have generally used the Congressional definition. For the purposes of the discussion that follows, we will stress that "ID theft" encompasses both sorts of crime.

4 Identity fraud and identity theft were codified in the Identity Theft and Assumption Deterrence Act of 1998, Title 18 USC Section 1028.

Whether they present the potential of account takeover or true name fraud, breaches of sensitive personal information[5] may result in substantial costs for the victim and enormous costs for the breached entity. Notifying people that their sensitive personal information has been breached can help to minimize the damage from the crime.

The logic behind notification is simple. If individuals are told that their sensitive information has been breached, they can monitor their accounts, take preventative measures such as opening new accounts, and be ready to correct any damage done.

Well before notification laws, many financial institutions had notification systems in place. These systems worked differently, especially in terms of the trigger for notification, than the "blanket notification" laws that are being considered in Congress or those already enacted in many states.[6] In light of the new bills being considered by Congress, it is worth asking not whether notification is worth it[7], but rather: how should a rational and effective notification system be structured?

DATA BREACHES AND IDENTITY THEFT

Estimates of Identity Theft Incidences

Before examining how a notification system should be structured, it's important to consider the scope of identity crimes and their trends. A number of recent studies estimate the scope of identity theft. The broadest is the FTC/Synovate survey of 4,047 adults conducted between March and April 2003. This study was followed up with a survey by Javelin Strategy and Research (which received input from the FTC during the formulation and analysis of the survey). While the Javelin study differs from the FTC/Synovate study in some respects, it is similar enough to allow a comparison of results. More importantly, in conjunction the two allow us to extrapolate some trends, albeit over a relatively short two-year period.

The 2003 FTC/Synovate survey estimates that, during the period April 2002 to March 2003, 9.91 million people were victims of true name fraud or account takeover in the United States, i.e., more than 4.5% of the US population. The survey further estimated that of these, 3.23 million people

---

5 There is some debate about how to define the phrase "sensitive personal information" but a reasonable approach was taken by California in the enactment of its security breach notification law. In this statute, sensitive personal information includes a combination of name and address coupled with a more sensitive item of information such as a person's social security number, financial account number and PIN or a driver's license number. Distinguishing between what is sensitive and what is not is a key to a rational regime for requiring notices be sent to consumers.

6 Arkansas, Connecticut, Delaware, Florida, Illinois, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Rhode Island, Tennessee, Texas, and Washington all possess blanket notification laws. Indiana's breach notification law applies solely to state agencies.

7 The question is worth asking, and Thomas Lenard and Paul Rubin, "*An Economic Analysis of Notification requirements for Data Security Breaches*", Progress and Freedom Foundation. July 2005 do try to answer it.

were victims of new account fraud. The damage from these crimes amounted to more than $52 billion and took up more than 295 million hours by victims to address. For most (63%), there were no out of pocket expenses.[8] Among those who were victims of credit card fraud, 75% incurred no out of pocket costs. Even 50% those who were victims of new account fraud suffered no out of pocket expenses.

Estimates of Data Breach Incidences

Estimates of the scope and scale of data breaches vary considerably, as do the types of information breached. "Breach" is not a monolithic term which means the same thing in all cases, breaches are fact-specific incidents. Some sound large and threatening, such as the loss of a customer backup table, but often the data that has been breached is either encrypted or in a format that is difficult for a criminal to decode.

How widely do breaches cover the population? A survey conducted by the Ponemon Institute and the law firm of White and Case suggests that 23 million people in the United States had "recently" been notified of a breach, not including duplicates.[9] This estimate is based on responses to the question whether the respondent recalls receiving a notification.

The Identity Theft Resource Center estimated that breaches involved unauthorized access to the personal information of potentially 56.3 million people in the first 9 months of 2005 alone (January through mid-September).[10] It should be noted and stressed that more than 70% of this rather alarming figure was accounted for by a single breach, that of CardSystems International.[11] Furthermore, the three largest breaches during this period account for 84% of all individuals whose information is open to potential misuse. It must be stressed that the presence of a breach does not reflect the actual risk posed by that breach (see below).

Identity Theft Crimes in the Context of Overall Crime Statistics

To reiterate, identity theft crimes are serious, and the incidences thereof require some new measures—whether legal, technological or market—to

---

8 FTC/Synovate, "*Identity Theft Survey Report.*" (Washington, DC: September 2003) www.ftc.gov/os/2003/09/synovatereport.pdf. p. 43 table Q30.

9 Larry Ponemon. "*National Survey on Data Security Breach Notification.*" Prepared for White & Case LLP September 26, 2005. www.whitecase.com/files/tbl_s47Details/FileUpload265/1199/Security_Breach_Survey.pdf

10 Identity Theft Resource Center, "*2005 Disclosures of U.S. Data Incidents.*" (10/3/2005) www.idtheftcenter.org/breaches.pdf

11 In this case, the breach of credit card account information certainly posed a risk to card holders, but the card issuing banks and their transaction systems (VISA and MasterCard) can mitigate this risk by monitoring account activity via robust neural networks which can spot transactions that are likely fraudulent, thus leading to the card being shut down. Further in this instance consumers were covered for all fraudulent transactions.

reduce victimization. The crimes must also be put into proper perspective. Consider identity theft crimes in the context of other types of commonly committed ones. The following table summarizes crime rates per 100,000 for identity crimes, violent crimes, and property crimes.

TABLE 1: ID THEFT, VIOLENT AND PROPERTY CRIME RATES, 2003 (per 100,000)	
ID Crime (of which)[12]	3,408
ID fraud (account takeover)	2,297
ID theft (true name fraud)	1,111
Violent Crime (of which)[13]	2,230
Aggravated Assault	460
Murder	100
Rape	500
Robbery	2,500
Simple Assault	1,460
Property Crime (of which)[14]	16,320
Burglary	2,980
Motor vehicle theft	900
Theft	12,440

Interestingly, as with other property and violent crime, identity crime rates have remained unchanged or have declined. A 2005 follow-up to the 2003 FTC/Synovate study by Javelin Strategy and Research found that the scope and scale of account takeover and true name fraud remained largely unchanged, despite impressions to the contrary. During 2004, an estimated 9.3 million people had been victims of account takeover and true name fraud, a slight decline from the 9.91 million estimated a year or so earlier. The total cost of fraud remained largely unchanged.

Of course, the scope and scale are substantial enough that, even unchanged, identity crimes remains a significant problem. However, there are other indications that things are improving. The Nilson Report, as Lenard and Rubin point out, shows that the costs of credit card fraud declined by 10% in 2004 from its 2003 level.[15] (Security and fraud detection systems are regularly improved, with companies having incentives to improve them, as they bear much of the costs. See below.)

---

12 FTC/Synovate, "*Identity Theft Survey Report*." (Washington, DC: September 2003) www.ftc.gov/os/2003/09/synovatereport.pdf.

13 Source: Department of Justice, Bureau of Justice Statistics "*National Crime Victimization Survey Violent Crime Trends, 1973-2004*", www.ojp.usdoj.gov/bjs/glance/tables/viortrdtab.htm

14 Source: Department of Justice, Bureau of Justice Statistics "*National Crime Victimization Survey property crime trends, 1973-2004*", www.ojp.usdoj.gov/bjs/glance/tables/proptrdtab.htm

15 Thomas Lenard and Paul Rubin, "*An Economic Analysis of Notification requirements for Data Security Breaches*", Progress and Freedom Foundation. July 2005.

The Javelin study also found that rates of identity crime (that is, incidents per 100 people) fell between 2003 and 2004 for both account takeover and true name fraud, from 2.6% (2003) to 2.28% (2004) and from 1% (2003) to 0.83% (2004), respectively.[16] Moreover, according to the Javelin study, the average time to resolve identity fraud and identity theft declined by 15% in 2004. This is not to downplay the seriousness of the crime, but it does suggest that measures in place already appear to be having some impact on the incidence of ID theft and ID fraud. These measures are increasingly being adopted and improved upon.

The following table summarizes the aggregate and individual costs of identity theft in 2003 and 2004, from the FTC/Synovate and Javelin studies.

TABLE 2: COSTS OF IDENTITY THEFT AND FRAUD (2003 AND 2004)

	2003	2004
Mean Cost per victim	$5,072[17]	$5,686
Total Cost	$51.4 billion	$52.6 billion
Existing Credit Card Fraud Rate ($)	2.6% ($28.4 b)	2.28% ($28.1b)
Existing non-Credit Card Fraud Rate ($)	1.1% ($12b)	1.15% ($14.2b)
New Account Fraud and Other Rate ($)	1.0% ($10.9b)	0.83% ($19.4b)
Mean Resolution Time	33 hours	28 hours
Average out-of pocket costs	$536	$652

It may be a consequence of the rising tide of identity crimes, but there are a number of indications that both preventative and corrective measures in the wake of identity crimes are becoming more effective. Information from Identity Theft Resource Center survey of victims suggests a similar trend. It found that the average time they spend as a result of the crime dropped from 773 hours in 2003 to 331 hours in 2004.[18]

Although it is probably better to look at these numbers in terms of the trend they suggest: in this case, over a 55% reduction in the amount of time spent to deal with a identity theft incidence. Why are we circumspect? The upper range of the time spent is listed to be 5,840 hours. In other words, 16 hours a day for 365 days—every waking minute for an entire year. When we eliminate the outliers, the averages are 435.6 in 2003 and 264.7 in 2004. Even with the outliers removed, these numbers may be inflated due to the idiosyncrasies of self-reported data.

16 Javelin Strategy and Research. 2005 Identity Fraud Survey Report. January 2005. Copy available at www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html.

17 FTC/Synovate figure adjusted for inflation.

18 Identity Theft Resource Center, "*Identity Theft: The Aftermath 2004.*" www.idtheftcenter.org/aftermath2004.pdf, Table 10, pp. 13-14.

Average lost earnings fell from $14,340 in 2003 to $1,820 in 2004, and expenses incurred also fell from $1,378 (2003) to $851 (2004)[19]. Again, the small sample size and the fact that respondents come to the survey rather than vice versa are facts that limit the usefulness of the findings. Nonetheless, it does help point to trends.

TABLE 3: IDENTITY THEFT RESOURCE CENTER SURVEY OF VICTIMS' COSTS (SELF-REPORTED)

	2003	2004
Hours Spent (without outliers)	773 (435.6)	331 (264.7)
Expenses	$1,378	$851
Earnings lost	$14,340	$1,820

Other measures also suggest a steady and persistent decline in financial fraud. Fraudulent purchases with credit cards accounted for approximately 0.18% of sales in the United States in 1992, when it peaked. By 2004, the figure had dropped to about one-third that, 0.06% of sales.[20] In 1992, as the information revolution got well underway, the financial and information industries began to invest more and more in fraud detection and prevention measures. Incurring most of the cost of fraud and having a deep interest in the consumer's trust in the financial system itself, these industries had and continue to have a strong incentive to do so. In considering state intervention, it's important to note that there are, and have been for a long time, private sector efforts to respond.

The measures have been extensive and evermore sophisticated. Beginning with the creation and maintenance of fraud databases, then moving toward better identity verification systems, industry has in recent years deployed statistical monitoring methods, neural networks, and other complex approaches that detect anomalies in economic behavior and other deviations from commercial patterns. Industry spent approximately $475 million in fraud detection technology in 2005; note, this does not include the costs of growing fraud detection and security departments or other measures designed to protect consumers. These facts are often overlooked in discussions of policy change. The measures initiated by the financial and information industries, motivated by preserving their market and by the fact that they incur costs from fraud, appear to be reducing instances of ID theft and ID fraud.

---

19 Identity Theft Resource Center, "*Identity Theft: The Aftermath 2004.*" www.idtheftcenter.org/aftermath2004.pdf, Table 10, pp. 13-14.

20 Source: Financial Insights, Bill Bradway and Sophie Louvel, "*Foiling the Fraudsters: Trends, Tactics and Tools.*" Presentation to Insights 2004 Client Conference. p.17.

Breaches and Identity Theft

Breaches vary considerably in scope and content. Reported breaches vary in size from a few dozen to the millions in some spectacular albeit rare instances. Furthermore, it is often the case that what information is breached is never quite known, at least not without catching the identity thief. The best that the firm and investigators are able to glean is what could have been potentially stolen. At times it may be unclear if there is even a breach.

Take, for example, the June 2005 case of the Kaiser Foundation Health Plan. The California Department of Managed Health Care (DMHC) fined Kaiser $200,000 for exposing private health information of approximately 150 people.[21] The health plan created a web site, containing information on the names, addresses, telephone numbers and lab results of patients, to be used as a testing portal. Kaiser did not receive the prior consent of the affected patients.

A month earlier, Time Warner reported that information, such as names and Social Security numbers, on 600,000 past and present employees of the company were lost while being shipped to an offsite storage facility. The ensuing probe did not find any unauthorized access or use.[22] The company paid for credit monitoring services for those whose information had been lost.[23]

In both of these cases it's unclear whether any breach had taken place. There was the possibility that the information was accessed by unauthorized people. Compare these two breaches with the well-publicized case of BJ's Wholesale Club. In early 2005, thieves monitored unencrypted data transmitted over BJ's wi-fi network. The system was furthermore accessible via a default username and password, and thieves gathered the credit and payment card information of BJ's customers. BJ's was alerted by card issuers that its customers were being victimized with fraudulent purchases in their name.[24]

The FTC investigation revealed that BJ's had not taken reasonable security measures to protect the sensitive information of its customers and had

---

[21] Linda Rosencrance. "*Kaiser Permanente division fined $200k for patient data breach.*" June 21, 2005. www.computerworld.com/printthis/2005/0,4814,102665,00.html

[22] It should be noted that the risk that breached data will be used in a crime increases over time. It is not uncommon for ID thieves to wait 12 or more months before making use of stolen information, such as credit card account numbers. However, increased public awareness of ID theft, the practice of notification, improved data security measures and more aggressive law enforcement make this practice harder for ID thieves. Jonathan Krim, "FDIC Alerts Employees of Data Breach," Washington Post, June 16, 2005.

[23] Cecile Daurat, "*Time Warner Reports Loss of Personal Data on 600000 Employees,*" May 3, 2005. Bloomberg News.

been negligent.[25] BJ's is party to a consent decree with the FTC that requires that they implement a comprehensive security system that will be subject to biannual external audits for the next 20 years.

Furthermore, the affected card issuers and financial institutions were sued to recover losses stemming from the breach. The total cost of this breach resulting from BJ's negligence—already substantial—could increase dramatically should things not go their way in court. This FTC enforcement action sent a clear signal to all entities handling sensitive financial information that certain minimum security standards must be in place. Note that had BJ's been defined as a financial institution under the Gramm Leach Bliley Act, it likely would have already been statutorily obligated to implement procedures very similar to the security requirements to which BJ's agreed in its consent order.

All of these—the cases of the Kaiser Family Foundation, Time Warner and BJ's—are breaches. Their character and impact, however, vary considerably. It's also unclear what share of total breaches each type of breach comprises. Comprehensive figures on breaches broken out by type are hard to come by. Further, not all breaches are necessarily reported.

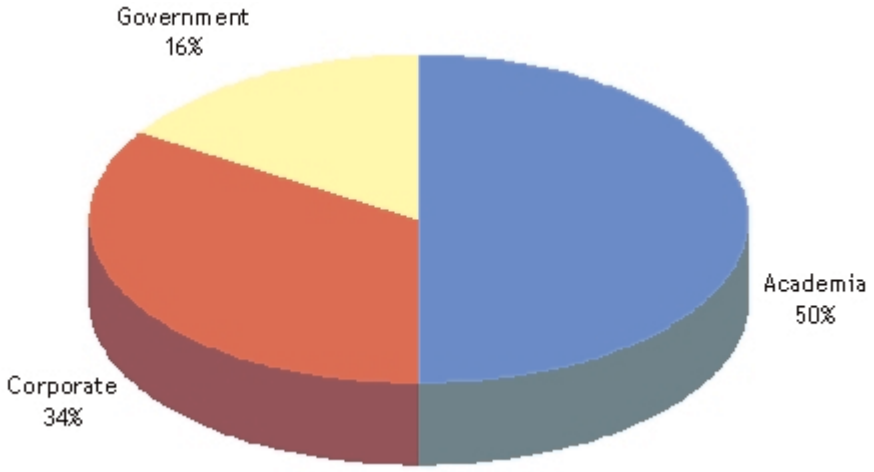
The Identity Theft Resource Center lists breaches that have been reported or discovered, and its list does allow us to examine where breaches are most frequent. The breaches listed by the ITRC were categorized by broad sector—government, academic, and corporate. Approximately half of all breaches listed for the period January 1, 2005 through September 15, 2005 took place in academic institutions. The information in university databases is often sensitive, comprising financial information, such as tax receipts, health information, and identifiers such as social security numbers.

---

24 Charles Kennedy and Kristina Hickerson, "*BJ's and DSW Cases Open a New Front in the War on Data Insecurity.*" Morrison & Foerster LLP, June 2005. www.mofo.com/news/updates/files/update02032.html

25 Thomas Calbum, "*BJ's Wholesale Club Settles FTC Data-Protection Complaint.*" Information Week. July 16, 2005. www.informationweek.com/story/showArticle.jhtml?articleID=164900340

FIGURE 1: SHARE OF REPORTED BREACHES BY SECTOR [26]
(JANUARY THROUGH SEPTEMBER, 2005) (N=112)



The private sector accounted for approximately 34% of all breaches, with government accounting for the remainder. Of course, governments and the private sector house larger databases than universities, so numbers of breaches may be a misleading indicator of the actual impact of breaches.

Notification can at most affect a very modest share of the total incidences of identity crime. The Javelin study was able to attribute 11.6% of identity crime incidences to information that was accessed/stolen on-line. An even smaller share of these incidents—potentially less than 5% of all identity crimes—are likely to be covered by proposed breach notification laws. [27] By contrast, in 68.2% of the cases, the information was accessed offline. (The remaining respondents did not know, refused to answer, or cited “some other way”.)

Identity Theft and Identity Thieves

As the identity crime becomes more serious, the probability that the victim will become aware of the criminal also increases. The FTC/Synovate survey found that while 18% of those who were victims of existing credit card

---

[26] Identity Theft Resource Center, "*2005 Disclosures of U.S. Data Incidents.*" (10/3/2005) www.idtheftcenter.org/breaches.pdf

[27] It should be kept in mind that "online" includes spyware and "phishing" (criminals posing as businesses). In fact, these two, which may not even be covered by proposed breach notification laws account for 6.9% of all incidents. If we assume that the 4.7% of incidences that would fall into the remaining cases where information is accessed "online" would be covered by breaches (an assumption which is far from warranted) and would therefore be people who received notices of the breach, then we see that notification would help to limit damage in a very small share of identity crimes. On the other hand, breach notification laws could potentially inform consumers as to the means by which their data was acquired, reduce the size of the "don't know" category, and therefore possibly drive the share attributable to breaches upwards.

fraud knew the thief's identity, 34% of those who were victims of new account (or other non-existing account fraud) could identify the perpetrator.[28] In fact, theft of account information or identity information by someone who is known to the victim (relative, friend, employee, or acquaintance) accounts for 20% of identity crimes, and, as a category in the broadest definition of identity theft, ranks second only to lost or stolen wallets, checkbooks, and credit cards.[29]

Yet, even if the scale of the problem of identity theft from breaches is overblown or hyped by the media, and even if those who are victims of identity theft from breaches are at time reluctant to take action, it remains a serious enough problem to consider some public solution.

NOTIFICATION A Possible Solution to the Potential Damage Caused by Breaches: Notification

Notification is dissemination of information to individuals that their personal information has been compromised when there is a reasonable likelihood of harm.

The rationale behind notification in the event of a data breach is simple. Giving notification to consumers that their information has been compromised allows them to immediately take protective measures, including reviewing their financial accounts and credit reports for fraudulent activity. The rationale for notification is also often grounded in the idea that because firms do not necessarily bear the entire cost of breaches, they may lack sufficient incentives to take measures to correct the breach or prevent future breaches. This latter notion requires additional scrutiny: a firm may, in fact, face significant costs beyond the value the actual fraud on the account less consumer and other third-party liabilities. Breaches pose risks to reputation and trust (see below), and by extension, market share and profitability. Finally, firms that have experienced breaches face significant litigation costs from class action lawsuits or governmental enforcement actions.

Most firms are not ideally situated to monitor a data breach victim's file for frauds on existing accounts let alone new accounts over which it has no access. Consumers, however, do have access to information about all of their accounts. There is good reason to believe that consumer monitoring of their accounts can reduce the damage from criminal misuse of their personal information. Moreover, generally only consumers place fraud alerts or file freezes on their credit file, measures that can reduce the

---

[28] FTC/Synovate, "I*dentity Theft Survey Report.*" Table Q14/Q15, p. 28.

[29] Javelin Strategy & Research, "*2005 Identity Fraud Survey Report.*" p. 8.

[30] On file freezes, see infopolicy.org/publications/freeze_final.pdf.

chance of malfeasance.[30] It should be noted here, that many consumers lack these rights at this point; a national standard for breach notification would empower consumers in this respect.

The Supply of Notification by the Market

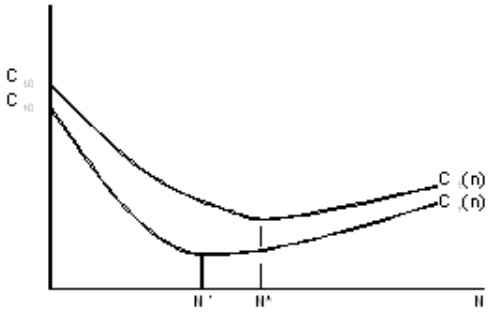
The question that remains open is: why is a legislative solution needed? If the market gives firms incentives to tell consumers that their information has been breached whenever one happens in order to limit damage that they will bear, intervention might be unnecessary. There are reasons to think that there may be instances when firms will not notify consumers of breaches even when there are benefits to doing so. First, a firm has an incentive to provide notification since it often bears the costs of the breach. There are costs that it does not bear, and instances when it is insulated from costs. A firm may not have an incentive to notify consumers of breaches when the cost of the notification exceeds the expected damage to *the firm*. That is, even if the costs of notifying a customer is smaller than the damage that will be mitigated, a firm has no incentive to bear this cost if the damage it will be spared is less than the costs of telling the consumer. Keep in mind, though, that market damage to firm is very broad; in addition to the direct damage done by identity fraud, it can incur reputational damage and lose potential business, it can be penalized by costly civil litigation or enforcement actions by states' attorneys generals and/or it can lose the future business of a client.

Yet, to the extent that the crime involves damage that is not borne by the firm (such as new account fraud, in which much of the damage is born by

---

[31] All else is not equal, however, as the number of notices can affect the size of preventable damage. See p. 15, "over-notification".

[32] To see how there could be undersupply, let C_{t0} be the total preventable fraud damage from a breach if the firm issues no notification and C_{f0} be the preventable damage associated with a firm. Notifications are ordered from most to least likelihood of identity fraud for the firm. With more notification (N), total damage is reduced as the individual monitors their accounts and credit reports, but only up to a point (N*). Where N > N*, over-notification detracts from the attention away from consumer and marginal fraud increases past the marginal cost of the notice. With respect to the costs of the damage associated with the firm ($C_f(n)$), damage is minimized at an "earlier" problem with less notification (N') than it is for total damage($C_t(n)$), which minimizes at N*. The reason why this is the case is that there may often be instances where information that is breached is difficult to be used for fraud on the accounts with the firm; this information comprises personal identifying information but not financial account information. That is, it can help to establish new accounts but not access or as easily access the account with the firm. Without a legal requirement, the market may well undersupply notice from the optimal level (N*). Of course a poorly structured notification requirement can overshoot that level.



others), it can have an incentive to undersupply notification. From the vantage point of society however, the optimal level of notification (all else being equal[31]) would be notification that eliminates all preventable damage, including that born by others, at least up to the point where the costs of additional notifications becomes larger than what we gain.[32]

Second, the firm may run the risk of damage as a result of notification itself. Reputational damage has been mentioned, but a firm also faces the risk of legal action (private and class), the penalties of which can exceed the value of the damage the firm incurs by doing nothing. In such instances, the firm may have a reason to avoid reporting a breach. Here the costs of notification may be substantial, especially to the extent that costs vary with notification—meaning the admission of a breach may bring additional costs. In this situation, the firm may find it rational to absorb the preventable costs to it and not issue notification of a breach.

In short, market forces may undersupply notification.

Of course, the problem of market failure does not automatically mean that state responses can necessarily remedy the situation. Required notifications can be structured in ways that reduce their effectiveness in minimizing potential damage. (See "Over-notification" below.) Market failure should not obscure the possibility of state failure or the dangers of regulation. Regulation should aim to make up the shortfall between an optimal level of notification and what the market will provide. Experience tells us that firms in the financial and information industries do bear extremely large shares of the costs of a breach. It should be stressed that firms, and especially those in the financial services and information industries, have been investing heavily in data security measures.

The increased attention being paid by firms to data security has resulted in more data breaches being discovered. This has had two effects. First, the growth in breach discovery has enabled firms to improve their understanding of security challenges and respond by bolstering their data security measures. Second, the dramatic growth in security investments and awareness that has produced the increased discovery of breaches has led to the misperception that the volume of data breaches, domestically and globally, are growing at an alarming rate. In fact, this is not verifiable. It may be the case that the number of breaches per thousand nodes on the Internet has remained fairly constant in recent years, but the ability of firms to track and identity anomalous or unauthorized access to databases has grown, thereby creating an impression of growth in data breaches. The reality is that more breaches are being discovered and prevented owing to the efforts of those seeking to protect their databases from intrusions.[33]

---

33 See Pricewaterhouse Coopers, "*Information Security Breach Survery 2004: Technical Report.*" www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf.

This trend is likely to continue as firms invest even more in protecting their IP and sensitive customer data and personal identifying information (including their own human resources data). Given that there is good reason to believe that greater and not fewer data breaches will be discovered in the near and medium terms, absent a properly calibrated trigger mechanism for data breach notification, other problems may arise—notably problems resulting from "over-notification".

The Limits of the Solution I: Over-notification

It is important to keep in mind that more notification is not necessarily better notification and may, in fact, be worse. The reason why is found in the fact that consumer responses to notification may be limited for a simple reason—limited attention. The requirement to notify may serve to actually reduce monitoring in cases where the chance of identity theft is significant, if it is structured poorly.

Herbert Simon, information theorist and Nobel Laureate in economics, was fond of pointing out the simple truism that information demands our attention.[34] Attention is the price we pay. He went on to note that a wealth of information produces a unique problem, how to allocate the limited attention we have over the ever-expanding sources of information. Attention is a scare resource, and in world of expanding information, more information can be a problem, rather than an automatic solution to the dilemma of ignorance, by turning individuals "off" to important messages that they otherwise would have noticed.

Recall that the benefit of notification in the wake of a breach is that a potential or actual victim would also monitor their account and, in so doing, help limit the damage done byan identity thief. That is, the attention given to an account by the person holding it helps to reduce the chances of account takeover and true name fraud. Notification can help to increase the attention that an individual gives his/her account, but only up to a point.

A breached firm prefers that the consumer be notified of the breach which is most likely to lead to fraud or theft, and then of the one second most likely to lead to identity fraud or theft, and so on, if each additional notice reduces the attention given to each breach. A consumer who receives notifications, over time, is likely to assume that any particular notification carries with it an average chance that the breach will result in fraud or theft. The broader the array of breaches for which notification is required, the lower the average chance that the breach of which the consumer is

---

34 Herbert A. Simon. "*Designing Organizations for an Information-rich World*", in Greenberger, M., ed., Computers, Communications, and the Public Interest. (Baltimore: John Hopkins Press, 1971). pp. 38-52, (Cited after reprint in: H.A. Simon, Models of bounded rationality. *Volume 2: Behavioral Economics and Business Organization* (Cambridge,Mass.: MIT Press, 1982.) p. 40.

informed will result in fraud. At some point, consumers begin to discount notices if the average likelihood that a breach will result in damage is very low. Recall, it is low to begin with.

Of course, the probability that a consumer will respond to a notification depends on a host of factors. All of these are likely to impact, to varying degrees, whether the consumer actually takes notice. Among the factors that increase the likelihood that a consumer will take notice is the "strength" or "intensity" of the notification itself. Though, if laws require notification in all instances, people may be likely to increasingly discount the notification, regardless of the media or content.

It should be pointed out that the volume of notification received by consumers (and thus the relative strength of a signal) depends on the thresholds for requiring that one be issued. If, for example, a virus attack requires consumer notification by law, even though the chances of identity fraud or, especially, identity theft are low, repeated notifications that are unaccompanied by any fraudulent activities may lead people to increasingly ignore them, including those that stem from breaches in which fraud is likely. In short, over-notification can be like the fabled cries of wolf.

The benefits of notification, all else being equal, depend upon its frequency. Its frequency, again, all else being equal, depends in turn on what occasions a notification— the breadth of the trigger, meaning how widely it encapsulates breaches of the system and the threshold for seriousness of the breach. Additionally, to the extent that notifications cover breaches that do not have a high chance of fraud or identity theft associated with it, the more likely it becomes that individuals will ignore them over time. By contrast, the more likely notices follow breaches with a high chance of fraud or ID theft, the more likely it is that potential victims will pay attention to notices. (This is of course an argument for a narrow trigger; see below.)

Over-notification runs the risk that consumer will treat notices that warn of a serious chance of identity theft as "noise". Already, there is evidence that data breach notifications are often treated in this way. The Ponemon survey of those who received a notification found that 39% of those who received them (or properly noticed them) initially thought it was marketing material of some form.

The Limits of the Solution II: Experiences with Notification

It should be mentioned that the effectiveness of notification assumes that all people notified will take the appropriate steps in response. These steps, as mentioned above, serve to reduce the damage done. Experience suggests that this assumption is often false.

---

[35] FTC/Synovate, "Identity Theft Survey Report." p. 50.

The FTC survey, as Lenard and Rubin note, indicates that 38% of victims take no action and do not even report the incidence to the credit grantor.[35] Only 43% informed credit grantors. Of those who have had new accounts opened in their name, that is, suffered the more serious type of identity crime, only 37% have contacted a credit bureau. More telling, of the 22% of victims of identity crime who contacted a credit bureau, 38% did not place a fraud alert—meaning, only 13.6% of victims placed a fraud alert. We can expect those whose information has been breached but who have not been the victim of an identity crime to do so more rarely. The reasons for why so many people fail to take action are unclear. Lenard and Rubin wrongly imply, we believe, that this response is rational since the chances of ID theft from breaches are so small.

Consumer non-action and limited action, especially in the wake of identity theft, may be based on other factors. 34% of victims surveyed by the FTC/Synovate knew who had stolen their identity.[36] Often these are friends or relatives, and as such, victims may be reluctant to take serious actions.

It's worth noting here that when asked how the notification could be improved, the plurality of respondents (37%) said that they would like a better explanation of the likely risks or harms from the breach.[37] Statistically speaking, these are small. It is unclear whether an accurate assessment of the likelihood of harm would encourage more effective monitoring.

ONE ISSUE TO BE CONSIDERED: REGULATORY FLEXIBILITY

While it may seem trivial at first glance, it is in fact, crucial to remark that concerns about how to best structure a breach notification can be rendered moot by an effective security program. In other words: no breaches, no notices. Clearly, consumers are far better served by having their data secure in the first place, than by being notified after the event of a breach. Because of the crucial interplay between information security and notification regimes, we now turn to a number of issues related to the regulatory environment for information security.

Data security assessments require that any inventory of data assets and vulnerabilities take into account the specific structure of that business. (In some cases, such as in subcontracting relationships concerning financial information, this is a requirement.) A firm's size, business model, its ownership structure, the components of business processes, the sensitivity of the personal data stored and transmitted, and technological platforms on

35 FTC/Synovate, "*Identity Theft Survey Report.*" Table Q14/Q15 p. 28.

36 Larry Ponemon. "*National Survey on Data Security Breach Notification.*" Prepared for White & Case LLP September 26, 2005. Table 5b, p. 9.

which those transfers occur all affect the approach that a firm takes to data security. As the sophisticated use of personal data continues to become more widespread across a host of industries, it is important that regulators demonstrate sensitivity to the needs of businesses with various business models and ownership structures. Sound regulation should aim to ensure that firms are not fettered in their ability to innovate in a competitive marketplace by unnecessarily inflexible security regulation.

There are a few issues that should be kept in mind when considering the economic and regulatory environment, and concern the diversity of business models of firms that house personal identifying information and how these data are protected. While these issues rightly focus on data security, as importantly, they caution against measures that threaten the vibrancy of the information economy. The well-regulated collection, use, and transfer of personal information have produced substantial benefits for the US economy. Moreover, the laws that currently regulate the information economy are products of debates, experience, and evaluations over decades. Conflating concerns—i.e., data security with data privacy—threatens to throw the baby out with the bathwater.

For example, in the financial services industry the use of consumer data is ubiquitous and indispensable: for account maintenance, risk assessment, and marketing. Regulators of the financial services industry have shown sensitivity to the dynamism in which these firms operate. Under the Gramm-Leach-Bliley Act (GLBA), the FTC was charged with describing the requirements of the Safeguard Rule of GLBA, the component of the act devoted to security concerns. As the FTC itself notes in its own commentary, the final rule is designed to be flexible. Financial services firms under the Act are required to design a "written information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue."[38]

The need for regulation to accommodate the flexibility of business organization is particularly important as firms grow, experiment with a host of organizational forms, and use specialized subcontractors in order to compete. These practices are common among smaller and medium-sized banks seeking to compete with larger financial services institutions.

Information can be processed in a number of organizational ways. The firm with which the consumer has the relationship can store, use and process the information. The information may be handled by a subsidiary, by a joint venture that has a separate managerial structure, or a sub-contractor. Any notification law must require the revelation of a serious breach while not biasing one organizational form. (The structure of liability plays a key role in determining bias; see below.)

---

[38] Gramm-Leach-Bliley Act, 15 USC 6801 Title 15, Chapter 94, Subchapter I , Sec. 6801. www.ffiec.gov/ffiecinfobase/resources/management/con-15usc_6801_6805-gramm_leach_bliley_act.pdf

The GLBA's safeguard rule, for example, takes into account the variety of business models, while limiting any influence it may have in biasing any one form over another. A notification requirement must as well.

Another issue to consider when crafting legislation designed to notify individuals in the event of the breach is firm size. Some firms that collect personal data may lack the capacity to comply with aspects of the law. For example, local grocers may maintain lists of their customers account information in order to extend them a line of credit. A law must not be so elaborate as to tax the resources of the smaller business that come under its jurisdiction. For a small firm, differences in costs stemming from the form of notification can be substantial. The firms may experience financial stress from notification levels that would not be felt by larger companies.

NOTIFICATION COSTS AND BENEFITS

Trivially, for notification to be useful, it should help to reduce the costs of fraud resulting from breaches, while incurring costs that are lower than what is gained by informing consumers. That is, the benefits of notification should exceed the costs of notification.

Total costs are the sum of two factors: the costs of notifying individuals of a breach; and the costs of actions taken by potential victims (including those other than identity theft victims) in response to a notice of a breach. The potential benefits are: any reduction or prevention of fraud and criminal as a result of earlier detection through consumer notification. As mentioned, the marginal benefits of notification are hard to judge, as firms have their own fraud detection systems (which are also coupled with their own notification systems). A strict accounting of the costs and benefits are therefore impossible, but Lenard and Rubin offer a useful assessment.[39]

Even with measurement challenges, it is worth considering the costs and benefits.

---

[39] Thomas Lenard and Paul Rubin, "*An Economic Analysis of Notification requirements for Data Security Breaches*", Progress and Freedom Foundation. July 2005.

[40] Although as noted earlier, it is best to examine these figures in terms of overall trends. There are good reasons--in particular, self-selection biases-- for believing that consumers may overstate the cost and time associated with identity crime incidents

[41] Larry Ponemon. "*National Survey on Data Security Breach Notification.*" Prepared for White & Case LLP September 26, 2005, Table 14, p. 16.
www.whitecase.com/files/tbl_s47Details/FileUpload265/1199/Security_Breach_Survey.pdf

Benefits of Notification to the Public

Above, it was noted that a victim of ID theft incurs costs of approximately $652.[40] From the perspective of someone's whose information has been stolen or otherwise compromised in a database as a consequence of a breach, the expected cost is much smaller. Lenard and Rubin point out that the chances that an account stolen from a database will be criminally used are small. Their estimates, based on fraud reports from VISA of compromised cards, range from 1% to 3%. The Ponemon survey of those who've received notification of a breach found that only 3% experienced identity theft.[41]

Roughly speaking, the expected cost of a breach to each person on the breached list is $20. Of course, many people are risk averse and do not wish to gamble. (Some do prefer to gamble, as it were, and do not take even modest measures such as placing fraud alerts on their credit files, as noted above.) This figure also does not include the cost of the victim's time dealing with the crime, though this can be easily approximated, and other more nebulous 'psychic' costs associated with being the victim of a crime.

The benefits of notification are sensitive to the time frame. The quicker a person receives notification, the smaller the costs they incur, on average, for reasons that are obvious. 67% of those who discovered the crime in less than 6 months after it began had no out of pocket expenses; by contrast, only 40% of those who discovered it more than 6 months after the beginning of the misuse had no such expenses.[42] It should be noted that such considerations must also compete at times with the concerns of law enforcement as well as the ability of lenders and consumer reporting agencies to handle a spike in customer service traffic (the latter could perhaps be addressed by staggering notices rather that having blanket notice requirements in the event of a large breach.)

But generally speaking, costs of identity crimes, if detected early, entail mostly only the loss of time for people. To the extent that notification leads individuals to identify misuse earlier, they directly benefit in the form of saving on out of pocket expenses.

Overall, if persons are engaged in reviewing statements, through a combination of consumer education, the use of free file disclosures, and the judicious use of breach notification, can the overall costs of identity theft be reduced? The FTC/Synovate survey found that the value of the theft in instances of identity crimes which were detected within 5 months exceeded $5,000 only in 11% of the cases.[43] In those instances in which

---

42 FTC/Synovate, "*Identity Theft Survey Report.*" Table Q30. p. 43.

43 FTC/Synovate, "*Identity Theft Survey Report.*" Table Q30. p. 43.

44 FTC/Synovate, "*Identity Theft Survey Report.*" Table Q38/Q39. p. 57.

the crime was detected in 6 months or more, the value exceeded $5,000 in 44% of cases. Again, 60% of the latter incurred out of pocket expenses, whereas less than 40% of the former did so. To the extent that notification can lead to earlier detection, consumers and businesses stand to save.

There are a number of ways to think about the issue of the benefits of notification. If notification leads to earlier detection, victims will save on out of pocket expenses, which average $500. Furthermore, to the extent that the costs incurred by the firm are passed on, individuals will save as well, but only to the extent that they respond to data breach notifications. Moreover, if reduced damage translates to less time needed to correct financial accounts and credit reports, victims can also save on the time needed to recover and restore their good names.

Even skeptics of notification are not prepared to suggest that the costs of notification outweigh the aggregate benefits. While there is much evidence to support skeptics' claim that the benefits are not as great as proponents of notification suggest, the benefits are, nonetheless, real and positive.

Costs and Benefits of Notification to Firms

The costs of notification depend in part on the delivery medium. Most state bills require that consumer be notified by mail. Bills currently pending before Congress also require that consumers be notified by mail. If the costs are significant, email, public notices, etc., may be substituted.

Mail notification has been estimated to cost approximately $2.00 per individual. Given that the chances of being a victim of identity theft as a result of breach of a database is 3%, firms will be spending $66 per victim. Of course, if notification can minimize damage by more than the costs, it's worth it. Above, we suggested that there is no foolproof method to determine each instance where notification is justified since notification becomes counter-productive after a certain point.

Additional costs emerge from the responses of those who've received notifications. These include opening a new account and/or issuing new credit and debit cards. To the extent that a small but sizeable minority of those whose information has been breached demand new accounts and new cards, companies may incur costs in excess of what is prevented by way of fraud.

It is nearly impossible to estimate what the expected response rate to any single notification effort *ex ante*; but it should be noted that nearly 30% of *actual* victims did not place a fraud alert on their credit reports.[44] What that means for predicting the response of *potential* victims who've been notified is unclear. Moreover, it's difficult to assess the costs without knowing the

scope of notification. The narrower the scope, the more likely the actions taken do minimize damage as these notifications would more likely cover instances for which the chances of identity crimes are the greatest. Rising costs come with notification, and preemptive actions, when the likelihood of identity theft is small.

Costs and Benefits to Third Parties

The costs and benefits of notification also accrue to parties other than breached firm(s) and the individual breach victims. To the extent that notification enables a person whose identity may have been stolen to take measures that limit new accounts in their name, companies in which the fraudulent accounts are opened stand to benefit in the form of lower fraud. To the extent that they pass on costs, all consumers will benefit as a result of reduced account service costs.

There are also costs to third parties that are generated by notification. This can take the form of monitoring, replacing credit cards, or establishing new accounts and closing old ones. On this issue the national credit reporting agencies (CRAs) deserve a specific mention. To the extent that those who are victims of identity theft or potential victims of identity theft may contact the credit bureaus to review their file disclosures, and will likely dispute any negative information that stems from the breach, CRAs can be caught by an unexpected flurry of inquiries and disputes. Additional costs stem from the actions of data subjects. These commonly include fraud alerts or credit file freezes.

Again, the aggregate additional costs depend in large measure on the likelihood that a consumer will respond to a breach notification and the costs associated with helping a victim or potential victim protect and restore their good name.

STRUCTURING A NOTIFICATION REQUIREMENT

A host of laws have been enacted in states—at the time of writing, 22—which statutorily compel firms to notify consumers in the event of a breach. More stand to be enacted. Additionally several bills on breach notification are before Congress, as the federal government considers national and pre-emptive breach notification.

Any breach notification law must consider: (i) what information is covered? (ii) under what conditions is notification required and under what conditions is it not? and (iii) what sanctions should be available in the wake of a breach? Related to these questions, in turn, is the issue of whether these are decided by lawmakers or regulators.

Restricting Notices to Breaches of "Sensitive" Information

Broadly speaking, there are two types of sensitive information in databases that may be used to perpetrate fraud. (i) There is information that is used to identify an individual. Identification is usually based on name, telephone number, and address in conjunction with someone's social security number, taxpayer identification number, or driver's license numbers, even a first pet's name. Name and address alone is largely public information and will not in and of themselves or together permit access to accounts, or enable a criminal to open a new one. Social security and driver's license numbers, by contrast, are "sensitive", when they are present in combination with a consumer's basic identifying information in that they can allow a criminal to pose as the victim or access the victim's accounts. (Additional informational used to identify an individual—such as mother's maiden name, first pet's name, etc.—are usually used as additions to the above for the purposes of further verification.)

(ii) There is information on a financial account that can enable a criminal to access and use the line of credit associated with it. Credit card numbers and their expiration dates, account numbers, or any other information that concerns a financial account and through the use of which a person can access the account are also classified as sensitive information.

Other information, e.g., of a purchase made, is typically not "sensitive" in the sense that it cannot be used to commit financial fraud or other criminal activity.

What specific elements count as sensitive is an empirical matter, measured by whether and the extent to which it helps a criminal access accounts or to establish new ones in the name of the victim. Moreover, its stability is also an empirical matter. Of course, given that the use of information is dynamic, it is hard to simply specify all elements that may be used for personal and account identification. Neither is it constantly in flux. There is sufficient stability in the data used for identification. These issues speak to a crucial aspect of breach notification, who specifies what information is "sensitive" and therefore covered by the law.

Two issues that have been considered are: (i) whether the data elements deemed sensitive and covered by the notification requirement should be specified in law or by regulatory rulemaking; and (ii) whether the covered information should be defined expansively or narrowly. If the system was far more dynamic than what is actually found, and if new data fields were being used for personal and account identification frequently, an argument could be made that the sacrifice involved in removing the issue from Congress would be worth it. That sacrifice is the fact that the specification of the elements establishes the domain to whom the law applies to—by democratic convention a prerogative that belongs to elected legislators and

not unelected regulators. Given that the system is relatively stable, sensitive elements can be specified in law. Further, lawmakers can respond to any significant evolution of the system with subsequent amendments to the law.

Expansive definitions run the risk of requiring notification when chances of harm are small. Email addresses, generic account information and the like are insufficient to access accounts and/or open new ones, at least without access to sensitive account access information as well. Again, broadly circumscribing covered information runs the risk of diluting the effects of notification when it's most needed.

Broad vs. Narrow Trigger

Notifications of data breaches are triggered, or initiated, by a breach of personal information, clearly. The issues that remain for policy are: (i) a breach of what personal information, and (ii) by what type of breaches? For example, in so much as infection by a computer virus requires the unauthorized access to systems by the malicious code, it is a security breach in the broad sense of the term. If it does not alter, retransmit, or damage personal information, little is gained by notifying the consumer, at least if the point of notification is to limit the risk of fraud and mitigate the damage done by identity theft.

Bills before Congress vary widely on the trigger. At the narrow side of the spectrum, notification is triggered when the breach is reasonably likely to result in financial fraud, or other harm to the consumer. [45] At the broad end, notification would be triggered merely by the reasonable belief that the information was breached.[46]

The case for a restricted notification trigger, one that is limited to a significant chance of identity crime rests in the belief that notifications will be more effective if they are used only in cases in which the company determines that there is a high chance of an identity crime. Notification of breaches, which are unlikely to result in misuse can, as suggested above, lead consumers to treat all breaches equally. This can result in a slower response rate to all notifications over time and thereby losing the benefits of a notification regime.

Regular review seems especially necessary for the more serious forms of identity theft, such as new account fraud, which take longer and more regular monitoring. Nearly 40% of "new account and other" fraud (as opposed to existing account fraud) required 3 or more months to resolve (Synovate, 26). Company notification accounted for the way in which the theft was discovered more than 25% of the time (Synovate, 39).

---

[45] For example, H.R. 3375

[46] Energy and Commerce committee draft.

Companies, as the principal bearers of the costs of identity theft, monitor account activities regularly in order to reduce their losses. They can only monitor fraud on their own accounts. Their capacity to monitor new accounts is largely non-existent, and monitoring of an individual's "name" can really only be done by the individual. This, counter-intuitively, argues for narrower notification, restricting it to instances in which a person faces a significant risk of identity theft. Less frequent notifications are more likely to attract attention, and attention to activities in the victim's name is precisely the objective of notification.

One further restriction on triggering a notification should be considered: the form that sensitive information happens to be in when it is stolen. Specifically, if the information is in an unreadable and unusable form—for example, if it is encrypted and stolen without the key—there may be no need to inform consumers of the breach. The California notification law (California's SB 1386) has already set this precedent and covers only unencrypted personal information.

The rationale for this *safe harbor*, restricting notification to the breach of sensitive information, and limiting that notification to instances when it is accessible and usable, is simple. Companies, third parties, and the potential victims themselves are primarily concerned about minimizing harm. As mentioned, attention must be turned to those instances in which harm is likely. The level of sensitivity of the information provides a first filter of whether the unauthorized access can lead to harm, so as to not expend attention. As both the FTC/Synovate survey and the Ponemon survey suggest, consumers already often have trouble recognizing notices as important.

A second rationale for the safe harbor(s) for encryption and truncation rests in the fact that it provides incentives for firms to adopt these measures, and commercial level encryption in the financial services sector is often quite stringent and difficult to crack. A safe harbor—with adequacy levels established by regulators[47] —can help to generate incentives to adopt security technologies across the economy. In this manner, a safe harbor provision for notification can help to prevent harmful breaches.

Private and Class Right of Action

A larger and more thorny issue is whether a private and class right of action should be excluded and whether enforcement should be left solely to law enforcement and regulators. The issue is thorny for obvious reasons.

The argument for a private and class right of action is, of course, that it will serve as a disciplining device and create incentives for firms to notify

[47] Of course, the level of adequacy should not impose unreasonable costs on the firm.

consumers in the event of a breach. Failure to do so can result in substantial loss to any firm found negligent by a court of law.

The argument for excluding a private and class right of action lies in the fact that the nature of the notification regime may create a strong incentive for frivolous suits. An effective notification regime would require that individuals be informed that the data has been breached in instances when the data is sensitive and where the breach can reasonably be interpreted to lead to harm. Much of this is a grey zone. Furthermore, in many cases, harm is difficult to directly tie to a breach. The decision not to notify—if law is already specific about instances (combinations of information) in which notification is mandatory and therefore non-notification criminal—in grey zones will be made in good faith. The danger of private and class action rights in these instances can lead to divergent responses. Some firms will simply over-notify, and the share of notices that are "noise" will increase, reducing the chance that notices will reduce harm—presumably the intention behind notification in the first place.

A RATIONALE FOR FEDERAL EXEMPTION

An Exemption for Existing Notification Policies

A number of state laws have exemptions for pre-existing notification policies, if these policies are consistent with the objectives of the law.[48] There are reasons for such an exemption. Firms with existing notification policies have designed them as a result of experience, testing and planning. These policies are intended to minimize harm as they relate particularly to the personal data kept by and business practices of the firm. To that extent, they are likely to be far more effective in reducing harm than the blanket requirements of the law.

While it makes economic and legal sense for the federal government to require notification (as argued below) and to specify the conditions, methods and content of notices for firms which have no policy in place, forcing these general purpose notice requirements on firms that already have notification policies in place is likely to produce a less efficient and effective system. A federal law should therefore include an exemption for those companies with notification policies that are consistent with its objectives.

As of April 2005, 23 states passed legislation requiring consumer notification in the event of a security breach of their personal information during the year. Including the California 2003 law, 24 states require notification in the event of a breach of personal information. Others introduced bills in 2005 and 2006 requiring consumer notification in the

---

[48] For example, Louisiana Act. No. 499, §3074 section, F, www.legis.state.la.us/billdata/streamdocument.asp?did=320093; Arkansas Act No. 1526, Section 4-110-106. www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf

event of a breach. Congress is also considering breach notification, and, furthermore, is considering pre-empting state laws. Which approach—national or state—is preferable depends on the mechanics of the issue.

The argument that some analysts have put forward that different state laws will result in a practice in which a company adheres to the most stringent one, or to the most stringent provisions in the varying laws is not necessarily true. With preemption debates, the metaphor of "floors" and "ceilings" are common, meaning whether state laws can drop "below" or can rise "above" the federal law. The metaphor is misleading at times because it presumes that actions are ordered on a continuum along which states choose a point. For example, notification periods can vary, but they can be ordered. If one state requires notification within 60 days of a breach discovery and another within 90, both state laws can be met by notifying within 60 days.

If one state requires that individuals be notified within 60 days of a breach and another requires that notification be held off if law-enforcement requests a delay, and if in these circumstance law-enforcement does indeed ask for a delay, then no single action can satisfy both sets of laws. The example is not merely hypothetical. While nearly all states allow for a reasonable delay for notification—usually "consistent with the needs of law enforcement" or "to determine the scope of the breach…and to restore the integrity of the system", the Illinois statute does not.[49] In a state-based notification regime, firms will not be facing so much a floor or a ceiling as a complicated maze.

The most common argument against a pre-emptive federal law is that it inhibits a process that amounts to many experiments being run. Experimentation at the state level allows multiple approaches to be "tested", as it were, and over time, we can see the effects of different forms of a policy. The best elements can then either be adopted by the states or be adopted in a federal law. Allowing states to experiment is taken to especially work well in new issue areas, where there is little experience in regulation and law enforcement, and data security and consumer expectations to data security are taken to be such a new area.

Then, state regulations can vary so widely as to impose unreasonable burdens on companies. The categories of information contained by the laws can be quite different. Some may include extensive and broad categories of data. Some may not require a significant risk of identity theft or identity fraud.

[49] Illinois General Assembly, Public Act 094-0036
www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036

TABLE 4: STATE NOTIFICATION LAW REQUIREMENTS AND ASPECTS

State	Likelihood of Harm or Specified Personal Information as Trigger	Delay for Law Enforcement	Delay to Restore Security	Time Limit	Safe Harbor for Pre-existing Notification Policy	Private Right of Action Allowed
Arkansas	X	X	X		X	
Connecticut	X	X	X			
Delaware		X	X		X	
Florida	X	X	X	45 Days		
Georgia		X				
Illinois			X		X	
Indiana		X	X			
Louisiana	X	X	X		X	X
Maine		X	X			
Minnesota		X	X			X
Montana	X	X	X		X	
Nevada		X		30 Days		X
New Jersey	X	X	X		X	
New York		X	X			X
North Carolina		X	X			X
North Dakota		X	X		X	
Ohio	X	X				
Pennsylvania	X	X			X	
Rhode Island		X	X		X	
Tennessee		X	X		X	X
Texas		X	X		X	
Utah	X	X				X*
Washington	X	X	X		X	X

* Does not create a private right of action, but does not affect private right of action under other laws.

It is commonly noted that these inconsistencies impose a cost on business. Where possible firms will opt for the most stringent measure in order to streamline the requirement and reap savings from scale economies. In the instance of notification, this response by firms may be the best they can do, but it does risk reducing the overall efficacy of notification. The most stringent law, or the amalgam of most stringent provisions, will produce a practice that results in over-notification.

Sound legislation must account for the fact that identity take over is a class of crime for which victimization is severe, costs are born largely by the victim, and where correction can be a lengthy endeavor.

CONCLUSION: BUSINESS ACTIVITY, NOTIFICATION, AND ERODING TRUST

There are good reasons to require notification. As mentioned above, the market may undersupply notification because there are instances of identity crime for which the breached entity does not bear the bulk of the costs and therefore has little incentive to notify potential victims. However, the peculiarities of informing people—the problem of attention—cautions against a broad notification requirement, at least if the objective is to minimize harm and overall losses from breaches. Notification of data breach victims when the likelihood of identity theft is significant can best capture the attention of those whose attention is most needed, the potential identity crime victims.

---

[50] Larry Ponemon. "*National Survey on Data Security Breach Notification.*" Prepared for White & Case LLP September 26, 2005, www.whitecase.com/files/tbl_s47Details/FileUpload265/1199/Security_Breach_Survey.pdf

There are also larger issues implicated in notification, issues beyond identity crime. In structuring any notification regime, it is important to remember that the well-being of the economy depends in large measure on trust between consumers and those with whom they have commercial and financial relationships. Even as the trends indicate that greater attention is being paid to cyber-security with greater concern for identity fraud and identity theft, it is unlikely that breaches will be completely eliminated.

It should also be kept in mind that the probability that any single breached account will be misused is small. Estimates range from 1% to 5%. (See below). Notification, while ignored by some, will over-alarm others. According to a survey of data theft victims by the Ponemon Institute "over 58% of respondents believed that the breach decreased their sense of trust and confidence in the organization reporting the incident. Over 86% of the subjects are concerned or very concerned about how the data breach incident will affect them."[50] About 20% of respondents have discontinued the use of services and another 40% were considering the leaving.

A larger worry is that consumers will distrust not merely the firms but electronic media and online systems, which have served to make the economy more vibrant—even though breaches of electronic and online systems, as mentioned, account for a very small share of fraud.[51]

To some extent, "exit" serves to discipline firms and acts as a feedback to have them pay more attention to their data security systems. On the other hand, if poorly structured, a breach notification law also can provoke flight by suggesting to people that their information is less safe than it in fact actually happens to be. To the extent that notification alarms people more than the likelihood of misuse warrants, notices run the risk of eroding trust in the system, that is, the system upon which much of this society's economic activity is based.

The contribution of data flows to economic growth is clear and well-established. Notification laws that are not well-calibrated run the risk of hampering this system. Therefore, any measures which would serve to weaken the bond of trust between individuals and commercial and financial institutions—such as would be the case with a notification regime predicated upon a broad trigger mechanism—should be avoided at all costs.

---

[51] To recall, the Javelin study was able to attribute 11.6% of identity crime incidences to information that was accessed/stolen on-line. Furthermore, if spyware and "phishing" (criminals posing as businesses) are excluded since they will not be covered by breach notification 4.7% of incidents can be generously traced to breached databases.

100 Europa Drive, Suite 431
Chapel Hill, North Carolina, 27517 USA
Phone: 919 338 2798
Fax: 212 656 1732
http://www.infopolicy.org

06/06