



January 19, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Taskforcecomments@idtheft.gov.

Re: Identity Theft Task Force, P065410

To Whom It May Concern:

The Consumer Data Industry Association (CDIA) appreciates the opportunity to comment.

CDIA's members play a key role in assisting consumers, businesses and governments of all levels in managing the risks posed to customers when there is a data breach. They are also the leading providers of technologies which prevent identity theft and fraud across a range of industries. Our members' also produce leading-edge direct-to-consumer file monitoring products which help consumers themselves to stop fraud and limit the damage caused by criminals.

GENERAL COMMENTS

Before we address the specific questions raised by the request for comment, we would like to offer some general observations. These comments should help provide context for our answers, and address issues that we feel should be highlighted or addressed by the Task Force, but are not evident from the questions.

1. Balanced Approach

The tenor of the questions presented by the Task Force, and the fact that the Task Force is not seeking any input into certain areas, highlighted below, leads us to believe that the Task Force recommendations may not provide the President with a balanced picture about what is occurring regarding ID Theft. For instance, there are no questions regarding what industry is doing to combat ID theft and the success of these efforts. Further, the notice does not explore the causes of ID theft, and what trend-lines there may be regarding this crime.

CDIA believes that the Task Force needs to present the issue to the President in a way that provides him with a broad picture of the entire landscape regarding this issue, not simply focusing on what can be done to address this issue, but also what has been done. Without that context, his ability to make useful and effective decisions is hampered. To effectuate this suggestion, CDIA would suggest that at a minimum the Task Force should explicitly recognize: 1) the role that the private sector has played and continues to play in protecting consumers from identity theft; 2) the recent leveling-off, and slight decline in the incidence of identity theft crimes; 3) the lack of data tying security breaches to the crime of identity theft; and 4) the current data protection regimes already in place, such as the Gramm-Leach-Bliley Act, (GLB), the Fair Credit Reporting Act (FCRA), and the Health Insurance Portability Act (HIPPA), that already provide substantial protections to consumers.

Attached as Appendix A is a presentation CDIA made to the Council of Western Attorneys General which provides data which we believe would inform the thinking of the President.

2. Definitions and law enforcement prioritization

1090 Vermont Avenue, NW, Washington, D.C. 20005
202-371-0910 Phone 202-371-0134 FAX

CDIA also would urge the Task Force to take advantage of this opportunity to seek to modify the definition of “Identity Theft” to more accurately reflect the realities of the situation. Specifically, FTC Chairman Majoris has been particularly effective at dissecting the difference between ID theft and other forms of fraud, such as credit card fraud. In fact, the FTC’s tracking of consumer complaints parallel’s the Chairman’s approach to presenting the facts about identity theft patterns generally fall into the categories of “new accounts” versus “existing accounts.” However, when defining the incidence of ID Theft, the FTC continues to rely on a broader definition that includes other fraud. CDIA urges the Task Force and the FTC to utilize this report process as an opportunity to clarify the debate about identity theft, and to utilize the more accurate description that the FTC has utilized in testimony.

This definitional issue is more than just semantics - there are real consequences that can occur if all types of fraud are lumped together as “Identity Theft.” First, this overstates the problem, and potentially leads consumers to make bad choices over minimized threats. Second, such an equal prioritization leads to misallocation of scarce law enforcement resources away from the most pernicious crimes. Third, it does not properly inform the public policy process which can lead to poor outcomes which can result in hundreds of millions of dollars spent on required actions which have no appreciable effect.

3. The incidence of identity theft

As demonstrated by the statistics maintained by the Bureau of Justice Statistics (BJS) and the FTC, the incidence of identity theft— once the fastest growing while collar crime in America -- has been dropping over the last few years. CDIA believes that the recommendations to the President should acknowledge that progress, and should put these recommendations in context of what appears to be progress in reducing incidence of the crime.

4. The link between data breaches and identity theft

Based on the questions posed by the Task Force, and their emphasis on dealing with data breaches and security, there appears to be an implication that data breaches lead to identity theft. However, a number of studies and surveys have attempted to look at where thieves obtain the information that they use to commit identity theft, and they have generally found that data breaches are a not a significant contributor to the problem of identity theft. Studies from Javelin (included as Appendix B) and ID Analytics (press release included as Appendix C), for instance, indicate that data breaches are a minimal contributor to the incidence of identity theft. Therefore, CDIA would strongly recommend that the Task Force explore in some depth where thieves obtain the information that they use to commit ID theft - you can’t solve a problem unless you know the cause of it.

5. Role of the private sector

The private sector has spent literally billions of dollars on security, anti –hacking and phishing and other fraud related initiatives, and should be recognized by the Task Force for many of these successful initiatives. Therefore, CDIA would recommend that the recommendations to the President include a section highlighting the initiatives of industry, and the role that industry has played in keeping consumer information safe. We would also argue that the Task Force should highlight some specific industry initiatives, such as the ID Theft Assistance Center, run by the Financial Services Roundtable, and the role of credit monitoring services provided by CDIA’s members, to help consumers protect their credit reports from future attacks, and other initiatives.

6. The Importance of Data to our Nation’s Economy

This report could lead readers to believe that information is primarily a threat and not a benefit. We don’t believe that this is the intent of the authors but we strongly urge the Task Force to set the context of the value of information. Included in Appendix D is an example of the type of context readers need to fully understand that the free flow of information is more important today and inures direct benefits to consumers both financially and from an ID theft prevention perspective.

7. Who Bears the Burden in a Data Breach

As the Task Force is aware, most of the data breaches, and particularly the sizable ones, occur outside of the credit reporting agency (“CRA”) community, and generally even outside of the financial services community. For example, in a review of media coverage of security breaches, nearly 50 percent of entities were public agencies or educational institutions.

When a breach occurs, CRAs are often on the frontlines, dealing with consumers who may be victims. Consumer notices almost always suggest that the potential victims contact one or more of the CRAs, get a free copy of their credit report, and potentially place a fraud alert on their file. The customer service agents of the CRAs are thus a primary contact with potentially distraught consumers. In one case where 750,000 sets of personal identifying information were lost as a result of a stolen hard drive, one of our members estimated that the incremental cost of FCRA compliance went up by \$1.5 million. The burdens shouldered by the consumer reporting industry should not be underestimated in this process, especially since they are rarely in a position to pass on the cost of the breach to the entity which experienced it.

8. Focus on the Federal Government

The language of the President's Executive Order clearly focuses the Task Force on the federal government, as acknowledged in the second sentence of the Request for Comments. This prioritization is clearly reflected in the Interim Recommendations of the Task Force, which focus almost exclusively on activities that the federal government should take. However, many of the questions asked through this document relate primarily, and in some cases exclusively, to the private sector.

9. Legislative Language

CDIA would strongly recommend that the Task Force NOT include any specific legislative language in its proposal to the President. Instead, CDIA would recommend that the Task Force stick to broad themes and principals, such as those laid out in Appendix 5, CDIA's principals regarding Effective Data Breach Notification legislation. Chairman Majoras has done an outstanding job framing the issue through her numerous appearances before Congress, and we would urge the Task Force to utilize that positioning to respond to Congressional proposals as they move through the process, rather than proposing specific language at this juncture.

10. Report Language

Finally, CDIA strongly cautions the Task Force to be very careful in how language is used in presenting these recommendations – tone and implication can say a lot. For instance, in laying out the goals of the Task Force on pages one and 2 of the Notice, the language implies that industry and regulators are not doing enough in this area. Specifically, the language indicates that the business community must be provided with “*more* comprehensive and effective guidance” (emphasis added), implying that regulations and guidelines established by the OCC and others is not sufficient; the goals also imply that *all* parts of the private sector need to have their data protection operations “enhanced,” again implying that industry, across the board, is not doing enough now.

Instead, per our discussion above, the business community—financial services in particular-- has been very engaged on this issue, and it is not fair to the business community nor to the President to neglect to tell him a major part of the story regarding ID theft.

B) COMMENTS ON THE QUESTIONS RAISED BY THE TASK FORCE SOLICITATION OF COMMENTS

I) MAINTAINING THE SECURITY OF CONSUMER DATA

General Comments Regarding SSNs¹

CDIA generally supports efforts to restrict the public display of Social Security numbers. However, there are many appropriate and beneficial business-to-business uses of SSNs that must be preserved that don't involve the “public display” of SSNs.

CDIA members use SSNs to verify individuals through the unique identifier of an SSN in court and public records, among other things. This information is necessary in credit reporting and employment reporting situations because the SSN is needed to correctly align the record with the appropriate person.²

¹ Also see: *The Statement of Stuart K. Pratt, President and CEO, Consumer Data Industry Association (CDIA), Before the Committee on Banking, Housing and Urban Affairs, United States Senate, on The financial services industry's responsibilities and role in preventing identity theft and protecting the sensitive financial information of their customers.* September 22, 2005
1090 Vermont Avenue, NW, Washington, D.C. 20005
202-371-0910 Phone 202-371-0134 FAX

In the U.S. there are 42 million address changes each year, 3 million marriages and divorces with attendant name changes, and there are six million vacation and second homes. Additionally there are 4.5 million Americans who have one of two last names (Smith or Johnson) and 14 million who have one of ten last names. 26.6 million females have one of ten first names and 57.7 million males have one of ten first and last names. The SSN is the single best way to ensure accurate consumer reports, effective fraud prevention, and a safe public.

Following are examples of how SSN's are used to accurately identify individuals in making credit decisions and as a tool to help prevent fraud.

- **Credit Reporting/Granting.** Banks, retailers, automobile dealers, and other lenders need to make the most accurate lending decisions with a wide array of information about the borrower.³ Without access to SSNs about a consumer's potential liens, judgments, bankruptcies, or other data, the lender is taking a far larger lending risk. Larger risks mean less available and more expensive credit for all consumers.
- **Fraud Prevention.** Without SSNs to help separate "John Smith" the law-abiding citizen from "John Smith" the identity fraud perpetrator, credit reporting agencies, lenders, law enforcement and others would have a far more difficult time preventing fraud. The result of a loss of SSN verification could result in increased identity fraud for more consumers.
- **Employment Reporting.** Often times, for the safety of the public, certain institutions screen employees to ensure there is no criminal history. For example, a bank will screen employees to ensure that there is no history of embezzlement or forgery on the applicant's file. Day care centers screen employees to ensure there is not a charge of pedophilia. Security providers screen employees to ensure no charges of breaking and entering. Bus companies and hazardous waste haulers screen their drivers to ensure there is no DWI on the applicant's record. If SSNs cannot be accessed, it is much more difficult to get an accurate reading on an applicant's criminal record, causing harm to the general public.
- **Law Enforcement.** Consider the sample of 242 stalkers in Delaware between May 1992 and June 1994 by the Delaware Statistical Analysis Center. Further investigation found that these 242 individuals had "accumulated an aggregated history of 5,010 arrests and 9,295 charges."⁴ It is safe to presume that these charges and arrests transcended dozens, perhaps even hundreds, of different jurisdictions and it is impossible to think that requisite tracing, authenticating and identifying those with court records (criminal or civil) can be accomplished without full SSN access. It is credible to believe that failure to have full SSN access could cause significant public safety harms while gaining little if any appreciable benefit to those whose SSNs is being truncated.
- **Child Support Enforcement.** Enforcement agencies estimate that absent the SSN, they can only locate 50% of non-custodial, delinquent parents. With the use of the SSN and the ability to match data against private-sector databases, they can reach a high of 90% effectiveness.
- **Public Funds Protection.** The federal Unemployment Insurance (UI) Crossmatch Project was created to reduce fraud committed on employers and states. The UI Crossmatch Program, heavily dependant on SSNs, identified, in 1998, 4,289 overpayments with a dollar value of \$2.3 million in Pennsylvania and 2,558 overpayments with a dollar value of \$1.2 million in Texas. Between July and December of 1998, Georgia identified 1,147 overpayments with a dollar value of \$227,577 and between July and December of 1998; Utah identified 213 overpayments with a dollar value of \$126,058. Loss of SSNs for unemployment liens risks the public financial health of the state.

Due to the tens of millions of changes in consumer identifying information, which occur each year, the SSN is the essential, stable identifier for accurate records. Fraud prevention systems that are used to reduce the incidence of identity theft or to authenticate consumers in an e-commerce or bricks-and-mortar context will be rendered less effective. In order for consumer reporting agencies, employment reporting and residential screening companies to better fulfill their purpose and role under the

² Nationwide CRAs have also sought access to the SSA database to verify/confirm SSNs. Such a system would enable CRAs to "ping" numbers off of the SSA database to confirm that a particular SSN belongs to a particular individual. Such a system would not only enhance the ability of the CRAs to properly match files, but would assist them in their investigations of ID theft allegations.

³ Comptroller of the Currency John Hawke, Jr. testified before Congress in 1999 that information exchanges serve a "useful and critical market function" that benefits consumers and businesses alike."

⁴ Department of Justice Violence Against Women Grants Office, Stalking and Domestic Violence: Third Ann. Rep. 33-34 (1998) (citing Department of Justice National Violence Against Women Survey).

Fair Credit Reporting Act in assembling, evaluating, and reporting fair and accurate information about consumers, they must have unfettered access to SSNs.

1. Government Use of SSNs

CDIA agrees that the federal government should explore ways to minimize its utilization of SSNs for employee identifiers and other uses of SSNs where the number is displayed publicly. However, the Task Force needs to be cautious in dealing with public records which may contain SSNs, at all levels of government. Specifically, CDIA's members rely on the use of Social Security Numbers to "match" particular records, such as liens, tax records and other public data, to the "correct" consumer's file. Without CRA access to this important identifier, consumer files could become less accurate, as either the number of incorrectly matched files increases, or the number of times data is not able to be matched and not reported increases, or both.

2. Comprehensive Record on Private Sector Use of SSNs

We question the value of a new study attempting to catalogue all uses of SSNs in the private sector. Our reasons are several. First, the GAO has written numerous reports on SSN uses by government and the private sector and it is unclear what this new effort would accomplish. Second, the extraordinary focus on SSN uses in the private sector implies that SSNs are still a key identifier which operate on their own. (In fact, the Interim report of the Task Force even suggests that a Social Security Number, *by itself*, can open an individual up to ID theft – a statement that CDIA would dispute.) Section 326 of the USA Patriot Act and new amendments to the FCRA made through the FACT Act all speak to a new era in identity verification. The private sector is well out ahead of duties under laws when it comes to using identity verification tools to authenticate applications. Our members are the leading providers of identity verification and fraud prevention technologies. Our members are also leaders in key discussions about the future of identity management including participation in the ANSI-facilitated discussions and those held under the aegis of the Center for Identity Management and Information Protection (Utica College, Utica, NY).

Nevertheless, if such an additional study is undertaken, CDIA and its members would want to participate, as appropriate, so that the important role that Social Security Numbers have in complete and accurate consumer reports is clearly understood.

3. National Data Security Standards

It is our view that rational and effective national standards should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a "financial institution."

The statutory framework for safeguarding sensitive personal information established by the Gramm-Leach-Bliley Act (GLB, 15 U.S.C. 6801-6809) sets forth a well-suited approach for national data security standards. GLB's statutory framework for safeguarding sensitive personal information by financial institutions could be extended to cover sensitive personal information held by any person not otherwise defined as a financial institution. Under this approach, the FTC would promulgate rules for any non-financial persons just as they did under GLB. To ensure that there is absolute regulatory continuity between the applicable provisions of GLB and rules therein and new information security standards and rules, financial institutions which are compliant with their obligations under GLB should be deemed in compliance with any new requirements. Any new standards for non-financial entities should be substantially the same as those required by the GLB safeguard rule.

However, the Task Force must be cautious in its approach: we believe that it is entirely inappropriate to either reopen GLB, which has been in place for almost a decade; and it would be inappropriate to create a duplicative standard that would require regulated entities to comply with 2 or more separate standards.

Additionally, as explained in more detail above, CDIA does NOT believe that the Task Force should recommend specific legislative proposals to the President.

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

Consumers should receive notices when their sensitive personal information is breached and there is a significant risk of identity theft.

Some elements that such a national security breach notification regime should include are:

- **Effective Preemption.** In a transient society, it makes sense that security breach notification obligations occur uniformly regardless of which state in which the consumer may live. This is particularly true of unencrypted information stored electronically. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare, and can result in consumers receiving notices where there is little or no significant risk to them of identity theft.
- **Harm/Injury Trigger.** Before a company or government agency is required to notify potentially enormous numbers of people of a security breach, there ought to be some showing that the breach poses a significant risk of identify theft. If a company or government agency concludes that no such risk of identify theft really exists, despite the existence of a breach, there is no sound public policy reason to notify and simply scare people. Otherwise, as we've seen in the context of privacy notices issued pursuant to the current myriad of different state security breach notification laws, over-notification creates instead a very real risk of consumer ambivalence.

We believe that the general guidance provided by FTC Chairman Majoras in her testimony before a number of congressional committees regarding the appropriate "trigger" for a notice is on point. That is that notices should be sent when there is a significant risk of identity theft. A poorly structured trigger leads to over-notification, which erodes the effectiveness of each subsequent notice sent to a given consumer. If notices are not tied to events that truly pose significant risks they will be ignored by many consumers who may become anesthetized to the importance of them.

- **Law Enforcement Consultation Option.** Any legislation ought to recognize that, in the event of a security breach, if law enforcement feels that sending the notifications to consumers should be delayed so as not to adversely impact an investigation, the sending of the notifications should be delayed.
- **Notification of Credit Reporting Agencies.** Because CRAs are the entities that are most often thrust into dealing with a data breach, they should be notified whenever large numbers of consumers become subject to notification, so that they can prepare to provide a timely and appropriate response to any resulting inquiries. This notification will help ensure that the CRAs have enough staff available to deal with the incoming consumer calls, and that the agents have the correct information regarding the calls.

Specifically, that the national systems' contact information is consistently listed in notices going to consumers. Adding up even a few of the high-profile breaches which have taken place, it is easy to come up with tens of millions notices containing our members' contact information. Thus, we believe that when a breach results in more than 10,000 notices to consumers, the company that breached the sensitive personal information should:

- Notify each nationwide CRA of this fact and provide the estimated number of notices to be sent;
- Notify any other CRA whose contact information will be listed in the notice; and
- Confirm the contact information that should be used for each listed nationwide and other CRA. Our members report that there have been times when incorrect telephone numbers have been listed on notices.
- **Functional Regulation.** Where appropriate, enforcement should lie with the functional regulators, or the FTC for unregulated entities. A decision to prosecute by the Attorney General of the United States should trump any action by a State Attorney General that is based on the same facts.
- **No Private Right of Action or Class Action.**
- **Reasonable Compliance Obligations.** Any compliance regime should be reasonable and predictable, with caps on fines and damages.
- **Safe Harbor.** Companies should be afforded some form of safe harbor from security standard and breach notification lawsuits if they comply with safeguarding guidelines. In other words, compliance with the FTC Safeguarding Rule, for instance, should shield a company from potential lawsuits in the event of a breach. This would not relieve the company of a notification standard, but would shield them from potential lawsuits that may result from such a breach.

-

- **Scope Limited to Usable, Computerized Data.** Breach notification obligations should not apply to either data that cannot be used or read, whether through encryption or other means, or paper materials. The greatest risk of harm to the public lies in the unauthorized use/access to computerized data. There is no public policy reason to broaden coverage to include either paper or unusable data.
- **Sensitive Data Definition.** The scope of any notification obligation should be carefully defined, as in California law, for instance, so that it only targets sensitive data likely to cause harm if released without authorization. While there should remain an inherent obligation to provide security for any personal information over which a person or agency has custody, the obligation to trigger a notification regime should not attach unless there is a significant risk of actual harm.

Additionally, as explained in more detail above, CDIA does NOT believe that the Task Force should recommend specific legislative proposals to the President.

5. Education of the Private Sector and Consumers on Safeguarding Data
 - a) Consumers

CDIA agrees that a government-led national consumer educational campaign about how to protect your data, and what should be done in the event of a breach, could be useful. For instance, the educational campaign should start with all of the resources that are currently available from sources such as the FTC, the CRA web sites, and other sources.

However, the Task Force again needs to be very careful in how these items are discussed. Specifically, while there are instances where data breaches may lead to consumer harm, those instances are rare, as the studies included with these comments demonstrate, and the Task Force should not convey the sense that any and all breaches are cause for panic.

We also believe that the consumer education campaign should also address how to respond to a breach. Some elements that such outreach should include are:

- 1) check your credit report
- 2) consider obtaining a credit monitoring service
- 3) consider placing an initial Fraud Alert on your credit file⁵

Fraud Alerts were voluntarily established by CDIA's members in the mid-nineteen nineties. Our members have long believed that fraud alerts strike the right balance for consumers who wish to ensure that a lender is notified of their concerns about identity verification where they have already been or may become victims of the crime of identity theft. Consumers recognize that while these alerts can slow down credit approval processes, alerts do not stop a transaction and, thus, consumers can continue to actively seek out better financial products and services whenever they wish.

The FACT Act created two specific types of fraud alerts. Initial alerts stay on the consumer's report for a minimum of 90 days and will be placed on the report even when there is just a concern that a person might become a victim of identity theft. Creditors which receive this alert must take steps to form a reasonable basis that they have properly identified the consumer. Extended alerts are placed on the consumer's file when he/she presents an identity theft report. This alert remains on the consumer's file for a full seven years and it may include contact information for a consumer which can be used as part of the identity verification process. Most important to the codification of our members' voluntary fraud-alert practice was that the FACT Act tied the presence of the alerts to specific duties for the recipients. This tying of the CRA's duty to place such alerts with a corresponding duty for recipients to form a reasonable basis for identity verification had never previously been established and our members believe that this materially improves upon the fraud alert systems that previously existed.

⁵ Similarly, active duty personnel may want to consider having an **Active Duty Alert** placed on their file. These are similar to fraud alerts, but are available only to individuals who are serving in an active duty capacity for our armed services. These alerts remain on the service member's credit report for twelve months and, like fraud alerts, are tied to duties for recipients to take steps necessary to reasonably identify the identity of the applicant before approving the application.

- 4) Check with your bank and credit card issuers to see if there has been any unusual activity on your accounts, such as unauthorized charges, a change-of-address request or a request for additional or replacement cards. If so, instruct the financial institution not to honor any requests regarding your account without written authorization. Ask them to cancel your debit and/or credit card and provide a replacement card with a new account number.
- 5) If fraudulent activity is discovered, file a police report and send a copy to creditors or anyone else who needs proof of the crime. Also contact the FTC at www.FTC.gov for further assistance with resolving any outstanding issues.

b) Private Sector

With regards to educating the private sector, there are a number of useful activities that the Task Force could assist with, including, as discussed above:

- Further publicizing all of the consumer education information that is currently available on CRA, CDIA, FTC and other web sites⁶;
- contacting CRAs in the event of a breach.

III. Preventing the misuse of Consumer Data

As noted above, CDIA members play a significant role in helping lenders authenticate potential borrowers. As discussed, SSNs play a major role in assisting CDIA's members to perform that function.

IV. Victim Recovery

1. Improving Victim Assistance

We agree that mitigating the effects of the crime of identity theft and restoring a consumer are very important. These are tasks our members consumer relations teams handle every day, and many of our members have established specific identity theft units to help victims. This said, we are concerned about how the question of victim assistance is posited, and the implication that many or most victims have serious problems rectifying the harm brought by the crime. While serious problems exist in some cases where there is a particularly pernicious form of ID theft and are thus more difficult to resolve, we believe that many consumers, such as those who identify a transaction on a credit card billing statement or who are victims of some form of account takeover, are quickly taken care of. It is likely that the anecdotes, though instructive, are not illustrative of the level of service provided by the CRAs or the ease with which the average consumer is able to obtain corrections. In some ways our concern supports the general point that aggregating a broad range of crimes under the rubric of identity theft, leads to imprecision in discussions of solutions.

2. Making Identity theft Victims Whole

While CDIA agrees with this recommendation generally, we would urge the Task Force to ensure that the business community is not held jointly and severally liable for criminal activity if the perpetrator of the security breach is not found or judgment proof.

3. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes

It is not at all clear how this proposed program would operate. The FTC itself has acknowledged that they do not authenticate the claims of consumers who self-report data into the Sentinel system. Further, were a new identification document considered to be an identity theft reports as defined under the FCRA, then you will find a higher rate of false claims as some consumers attempt to obtain the ID document in order to delete accurate, but adverse information on their credit reports. We recognize that some consumers, such as those where a criminal record has been created in their name, are in need of unique solutions. We would urge caution in the creation of new systems. We suggest that the federal government should first review the ID theft

⁶ It is also useful to point out that under FCRA, consumers receive a summary notice of their FCRA rights, and those who suspect they are or could be victims of ID theft receive a summary of "remedying the effects of ID theft" when they contact the CRAs.

passport programs that are being developed in states such as Utah, Ohio and Montana to see how these operate and how effective such programs truly are.

4. Gathering Information on the Effectiveness of Victim Recovery Measures

a. Assess the impact of FACTA amendments

In working closely with the FTC and other agencies charged with implementing and enforcing the FACT Act, CDIA is under the impression that the agencies are constantly conducting an on going analysis to assess the effectiveness of the FACTA and rules under their jurisdiction. A separate assessment appears as though it would likely be a drain on agencies' resources to force them to conduct another, separate assessment.

In addition, there are still many rules that need to be implemented across many agencies. Having been intimately involved in a number of discussions and Rulemakings within many agencies, CDIA believes: 1) that the agencies are doing appropriate due diligence to implement the rules under their jurisdiction, and 2) that inappropriate political pressure from the Task Force may force the agencies to make detrimental decisions.

b. Conduct an assessment of State Credit Freeze laws

CDIA and its members generally feel that fraud alerts strike the appropriate balance between protecting and inconveniencing consumers.

There are currently 26 states that have enacted some form of file freeze law and another 15 states are likely to consider freeze proposals during the 2007 legislative session. CDIA and its members are working closely with State legislatures to adopt laws that are operationally consistent with that passed by California.

Though some file freeze provisions of state laws have been effective for years, our experience with them remains very limited. For example, we estimate that just a little over 20,000 California consumers have made use of the file freeze, even though the law has been in place for 3 years, and has been extensively covered by the press, with dozens of stories about file freezing appearing in newspapers across the country over the last year. With a population of more than 25 million credit-active Americans, this population of frozen credit reports yields no useful information regarding the individual consumer experience, except that the consumer "take" rate is very low. Further, most state laws are very recent enactments and, thus, we also have no experience with consumers moving in and out of states where the file can and cannot be frozen.

IV Law Enforcement: Prosecuting and Punishing Identity Thieves

1. Establish a National Identity Theft Law Enforcement Center

CDIA recommends that the Task Force confer closely with entities that perform these services in both the private and public sectors.

CDIA also supports the establishment of a uniform ID theft police report, as the Task Force has recommended in their Interim Report, and have started to implement. Such a standard will better enable victims to begin the recovery process, and could also assist law enforcement in tracking and prosecuting these crimes, particularly if they occur outside of their jurisdiction.

2. Ability of Law Enforcement to Receive Information from Financial Institutions

c. Discussions with CRAs

As the trade association which represents CRAs, among other entities, CDIA and our members are always willing to hold discussions with law enforcement regarding this issue – you do not need Task Force approval to call us.

5. Prosecutions of Identity theft

CDIA encourages the law enforcement community to increase the number of ID theft prosecutions. However, given our previous discussion about law enforcement prioritization, we would again encourage the Task Force and law enforcement to focus on the most egregious crimes and activities – notably focusing on new account fraud.

CDIA would also encourage a lowering of monetary thresholds if that is a significant impediment to bringing these cases. Specifically, CDIA has heard anecdotal stories about how prosecutors refused to bring cases because of a low monetary threshold, which discouraged law enforcement from even pursuing a case because the “the prosecutors would never bring it.” Such an attitude not only leaves consumers high and dry, and often makes it more difficult for them to clear their names and credit if there is no law enforcement activity, but in addition pursuit of a single case could lead to a broader ring.

6. Targeted Enforcement Initiatives

Again, CDIA generally agrees that law enforcement activity to go after identity thieves is a very useful activity. However, we caution the Task Force in its approach to (a) “unfair or deceptive means to make SSNs available for sale.” As discussed previously, business-to-business provision of SSNs should not be a target of this action, nor should the sale of public documents which may happen to contain a SSN.

7. Amendments to Federal Statutes and Guidelines Used to Prosecute Identity Theft Related Offenses

Again, CDIA generally supports strong law enforcement efforts to combat ID theft, and we are supportive of prosecuting employees who violate the trust of an employer to misappropriate information. However, we caution that such a statute should not extend to holding corporate employees criminally liable for acts of negligence that may have led to a breach at a company.

CDIA also has very serious reservations about making it a felony for employees of “data brokers” to sell customer information – this idea needs a lot more “meat” and a LOT more thought before it can be pursued, particularly if the Task Force is considering making whatever activity you are seeking to cover a felony offense:

- First, there is no definition of “data broker,” so criminalizing conduct by an employee of an undefined entity is likely overly broad and prescriptive;
- Second, presumably “data brokers” would only sell information obtained by other entities, (hence, the “broker” part of the definition.) Therefore, the entity likely does not have a direct relationship with a “customer,” so they could not obtain “consent” from them;
- Third, if the data is sensitive financial or health-related information, it is likely already covered through some pre-existing law, such as HIPAA or GLB; and
- Fourth, there needs to be some exception for publicly available information.
- Fifth, embracing this term, “data broker,” coined by media does not lend precision to the report. Many CDIA members are accused of being unregulated data brokers when nothing could be further from the truth. Our members are regulated by a plethora of laws and regulations including the FCRA, GLB, HIPAA, COPPA, the FTC’s DNC list, FDCPA, DPPA and more. The report should fully inform its audience of the extensive base of sectoral laws which regulate a variety of sets of sensitive personal information used for fraud prevention, risk decisions, security clearances, and debt collection.

7. Measuring Law Enforcement Efforts

As discussed previously, there is little data at all regarding how ID theft occurs and where the thieves obtain the information. CDIA believes that these are vital questions that need to be answered, not just by law enforcement, but by other agencies, as well, such as the FTC.

CONCLUSION

CDIA and our members certainly appreciate the work the Task Force has put into this effort. However, there are a number of significant issues that it appears as though the Task Force is ignoring, which must be included if the recommendations to the President are going to be balanced and fully accurate. Therefore, rather than rushing to finish this document, CDIA would strongly advise the Task Force to take your time and hold discussions about some of the issues raised in these comments.

Thank you again for the opportunity to comment – we stand ready to work with the Task Force.

Sincerely,

A handwritten signature in black ink, appearing to read "Stuart K. Pratt".

Stuart K. Pratt,
President and CEO

Appendix A

CDIA Power Point Presentation to CWAG



06 CWAG v1.ppt
(252 KB)

Appendix B

Javelin Study



617.RF_Data
eaches and Ident

1090 Vermont Avenue, NW, Washington, D.C. 20005
202-371-0910 Phone 202-371-0134 FAX

ID Analytics' First-Ever National Data Breach Analysis Shows the Rate of Misuse of Breached Identities May be Lower than Anticipated

Evidence Suggests that the Smaller the Data Breach, the Higher a Consumer's Risk

SAN DIEGO, CA, December 8, 2005—ID Analytics, Inc., the Identity Risk Management company, today announced findings from its detailed analysis of four data breaches involving approximately half a million consumer identities. As of now, the results reveal that few of the breached identities from the analysis appear to be misused for criminal financial gain.

A significant finding from the research is that different breaches pose different degrees of risk. In the research, ID Analytics distinguishes between “identity-level” breaches, where names and Social Security numbers were stolen and “account-level” breaches, where only account numbers—sometimes associated with names—were stolen. ID Analytics also discovered that the degree of risk varies based on the nature of the data breach, for example, whether the breach was the result of a deliberate hacking into a database or a seemingly unintentional loss of data, such as tapes or disks being lost in transit.

“The risk to consumers and businesses varies considerably based on the type and scope of the data breach, which is why we think assessing the degree of risk for a given breach is critical to determining the best next steps,” said Mike Cook, ID Analytics’ co-founder and vice president of product. “The good news is not only that we have technology that can measure the risk of a breach, but that we can actually distinguish which sets of breached data are actively being used to commit fraud.”

ID Analytics’ research makes it clear that identity-level breaches pose the greatest potential for harm to businesses and consumers due to fraudsters’ sophisticated methods for profiting from identity information, as compared to account-level breaches. Even so, the calculated fraudulent misuse rate for consumer victims of the analyzed breach with the highest rate of misuse was 0.098 percent—less than one in 1,000 identities.

“We feel strongly that this research provides meaningful evidence both for companies working to mitigate the risks that stem from data breaches as well as for elected officials working toward a legislative solution,” said Bruce Hansen, chairman and CEO of ID Analytics. “What’s more, we think this information can help consumers assess their relative risk if they have been a victim of a data breach.”

ID Analytics’ fraud experts believe the reason for the minimal use of stolen identities is based on the amount of time it takes to actually perpetrate identity theft against a consumer. As an example, it takes approximately five minutes to fill out a credit application. At this rate, it would take a fraudster working full-time - averaging 6.5 hours day, five days a week, 50 weeks a year - over 50 years to fully utilize a breached file consisting of one million consumer identities. If the criminal outsourced the work at a rate of \$10 an hour in an effort to use a breached file of the same size in one year, it would cost that criminal about \$830,000.

Another key finding indicates that in certain targeted data breaches, notices may have a deterrent effect. In one large-scale identity-level breach, thieves slowed their use of the data to commit identity theft after public notification. The research also showed how the criminals who stole the data in the breaches used identity data manipulation, or “tumbling” to avoid detection and to prolong the scam.

“Consumers need to know the level of risk that is posed if they are part of a data breach. While any data breach is cause for concern, consumers that have been impacted need guidance as to the degree of risk involved,” said Linda Foley, executive director of the Identity Theft Resource Center. “It’s not helpful for consumers to receive a generic letter in the mail telling them that they may or may not be at risk. We need to help victims of breaches understand when they need to be more vigilant and prevent them from being unnecessarily alarmed.”

Research Methodology

1090 Vermont Avenue, NW, Washington, D.C. 20005
202-371-0910 Phone 202-371-0134 FAX

This analysis was based on data breaches at four separate companies, covering approximately half a million identities. ID Analytics conducted the analysis over the past six months by analyzing this data against applications in its ID Network™, which comprises more than 3 billion identity elements contributed by its members. ID Network Members include the largest US industry leaders from across the credit card, wireless telecommunications, and instant lending industries. ID Analytics Graph Theoretic Anomaly Detection (GTAD®) technology was applied throughout this study to detect behavioral fraud patterns. ID Analytics' expert fraud analysts further qualified that selected cases of identity misuse were likely the result of specific fraud activity.

About ID Analytics, Inc.

ID Analytics is the Identity Risk Management company providing advanced analytic solutions that prevent identity fraud and manage identity risk across the customer lifecycle. ID Analytics' intelligent ID Network, the first and only real-time national network built exclusively to manage identity risk, makes it possible for organizations to calculate the risk associated with an identity and balance identity risk against profit. The ID Network is in use daily by over half the credit and retail card issuer market in the US, as well as leading wireless and online consumer finance companies. To empower consumers and to help more organizations in more industries to fight identity fraud, ID Analytics has channel partners in the bankcard, credit reporting and retail banking industries. ID Analytics, host of Identity 2006, the annual Identity Risk Management Conference Sept. 18-21, is based in San Diego with offices throughout North America and the UK.

For More Information Contact:

Stacy Peña
Rainmaker Communications
+1 (650) 965.2985
stacy@rainmakercommunications.com

Karen Stadelmeier
ID Analytics
+1 (858) 312.6244
kstadelmeier@idanalytics.com

ID Analytics and GTAD are registered trademarks of ID Analytics, Inc. ID Network is a trademark of ID Analytics, Inc.

The Economic Value of the U.S. Credit Reporting System

- *“The banking system is dependent upon fair and accurate credit reporting.”*
- *“An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character and general reputation of consumers.”*
- *“Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.”*

These excerpts from the “statement of purpose” of the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) are no less true today than when they were first written as part of the enactment of this law in 1970. In fact, it is a given that consumer spending and access to affordable credit is a key pillar of the U.S. economy

For years many have intuitively acknowledged the value of the U.S. credit reporting system, however in the past decade empirical measures and studies have demonstrated just how profoundly important credit reporting really is to our economy as a whole. Consider the following:

- “Transparency of consumer credit data is the foundation of consumer credit in the US. Outstanding consumer loans exceed both government debt and corporate debt in the US, and constitute sixty percent or better of US gross domestic product (GDP). The consumption consumer credit comprises two thirds of US GDP. Perhaps most important is the fact that people and capital are relatively more mobile in the US serving to minimize economic dislocations in a more competitive global economy.”⁷
- “Securitization, largely driven by consumer loans, numbers in the US trillions of dollars, but is not common outside of North America. Because of Fannie Mae, and other US sponsored conduits to the secondary market, mortgages in the US are estimated to cost as much as 200 basis points lower.”⁸
- “Credit bureau data on consumer borrowing and payment behavior has become the cornerstone of the underwriting decision for consumer loans in the United States. Armed with the most comprehensive consumer payment histories on the planet, creditors apply statistical scoring models to estimate an individual's repayment risk with remarkable accuracy.”⁹
- “Perhaps most significantly, credit bureau data has made a wide range of credit products available to millions of households who would have been turned down as too risky just a generation ago.”¹⁰
- “In 2002, the Federal Reserve estimates that homeowners were able to extract some \$700 billion of accumulated equity from their homes, prompted by the lowest interest rates in 35 years, according to the Federal Reserve Board.”¹¹
- “Between 1983 and 2001, the share of families with home-secured debt rose from 36 to 45 percent. Over the same period of time, the percentage of families who owned their homes increased from 60 to 68 percent.”¹²
- “Previously underserved groups have greater access to credit. The percentage of households in the lowest income quintile with a credit card has increased from 2 percent in 1970 to 28 percent in 2001. During this same period, the percentage of African American households with credit cards has more than doubled, from 23.6 percent to 55.8 percent.”¹³

There is no doubt that the U.S. credit reporting system and the uniform national regulatory framework established through the FCRA, are the key to our consumer-spending based economy. In fact, the World Bank and the United States Agency for International Development are both working to replicate the success of the U.S. credit reporting system in other developing countries.

⁷ Kitchenman, Walter., U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns., Pp. 5 (1998).

⁸ Ibid. Pp. 8.

⁹ Barron, John., Staten, Michael., The Value of U.S. Credit Reports: Lessons from the U.S. Experience. Pp.2 (2000).

¹⁰ Ibid.

¹¹ Turner, Michael., The Fair Credit Reporting Act: Access, Efficiency & Opportunity. Pp. 8 (2003).

¹² Ibid. Pp. 6.

¹³ Ibid.

Breach Notification Principles

- **Effective Preemption.** In a transient society, it makes sense that notification obligations occur uniformly regardless of which state in which the consumer may live. This is particularly true of unencrypted information stored electronically. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare. None of the major bills introduced thus far adequately addresses preemption.
- **Harm/Injury Trigger.** Before a company or government agency is required to notify potentially enormous numbers of people of a security breach, there ought to be some showing that the breach poses a significant risk of actual harm or injury that might lead to identify theft. If a company or government agency concludes that no such risk of identify theft really exists, despite the existence of a breach, there is no sound public policy reason to notify and simply scare people. Otherwise, as we've seen in the context of privacy notices issued pursuant to the Gramm-Leach-Bliley Act, over-notification creates instead a very real risk of consumer ambivalence.
- **Law Enforcement Consultation Option.** Any legislation ought to recognize that, in the event of a security breach, companies may choose to notify the appropriate federal enforcement authorities/functional regulators, especially where illegal activity is suspected. They should nonetheless retain the right to make on-the-spot decisions about whether or not to notify consumers whose identities may be at risk. Credit Reporting Agencies should be notified whenever large numbers of consumers become subject to notification, so that they can prepare to provide a timely and appropriate response to any resulting inquiries.
- **Functional Regulation.** Where appropriate, enforcement should lie with the functional regulators, or the FTC for unregulated entities. A decision to prosecute by the Attorney General of the United States should trump any action by a State Attorney General that is based on the same facts.
- **No Private Right of Action or Class Action.**
- **Reasonable Compliance Obligations.** Any compliance regime should be reasonable and predictable, with caps on fines and damages.
- **Safe Harbor.** Companies should be afforded some form of safe harbor from lawsuits if they have instituted reasonable internal security and notification procedures.
- **Scope Limited to Non-encrypted, Computerized Data.** Breach notification obligations should not apply to either encrypted data or paper materials. The greatest risk of harm to the public lies in the unauthorized use/access to computerized data. There is no public policy reason to broaden coverage to include either paper or encrypted data.
- **Sensitive Data Definition.** The scope of any notification obligation should be carefully defined so that it only targets sensitive data likely to cause harm if released without authorization. While there should remain an inherent obligation to provide security for any personal information over which a person or agency has custody, the obligation to trigger a notification regime should not attach unless there is a significant risk of actual harm.



JAVELIN STRATEGY & RESEARCH

Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses

August 2006

Telephone:
925.225.9100

Fax:
925.225.9101

Address:
4309 Hacienda Dr., Suite 380
Pleasanton, CA 94588

Email:
inquiry@javelinstrategy.com

Web site:
www.javelinstrategy.com

Overview

Misunderstanding data breaches and their effect on identity fraud may lead to incorrect guidance to consumers, mistakes regarding protective measures companies employ, and overly-burdensome legislation. Armed with facts, industry leaders must ensure that the data breach “cure” is not worse than the affliction. This report is the first ever to show the actual impact that data breaches have on known-cause cases of identity fraud.

Primary Questions

- How does misunderstanding of data breaches and their effect on identity fraud impact businesses, government, and consumers?
- How many individuals are being notified that they were a victim of a data breach and how likely are these individuals to become a victim of actual fraud?
- How likely will a typical data breach cause identity fraud (based on nationally representative survey data)?
- What is the current status of data breach legislation?

Findings and Analysis

While public data breach notifications in 2005 reached into tens of millions of accounts, total annual identity fraud only increased four percent. The large number of data breaches and the publicity they have received has created the misperception that *fraud resulting from data breaches* is prevalent. Javelin data indicates, however, that only six percent of all known identity fraud is generated from data breaches. The percentage of consumers who go on to suffer a fraud as a result of a data breach is only 0.8%, or eight out of every 1,000. Strict automatic data breach notification laws “regardless of risk” to the victim will saddle businesses with costly and unwarranted requirements, while providing little protective value to consumers.

Audience: Financial institutions, online banking and risk/fraud divisions

Author: Mary T. Monahan, Editor/ Analyst

Contributors: Bruce Cundiff, Senior Analyst
James Van Dyke, President
Stephen Matava-Knighten, Research Associate

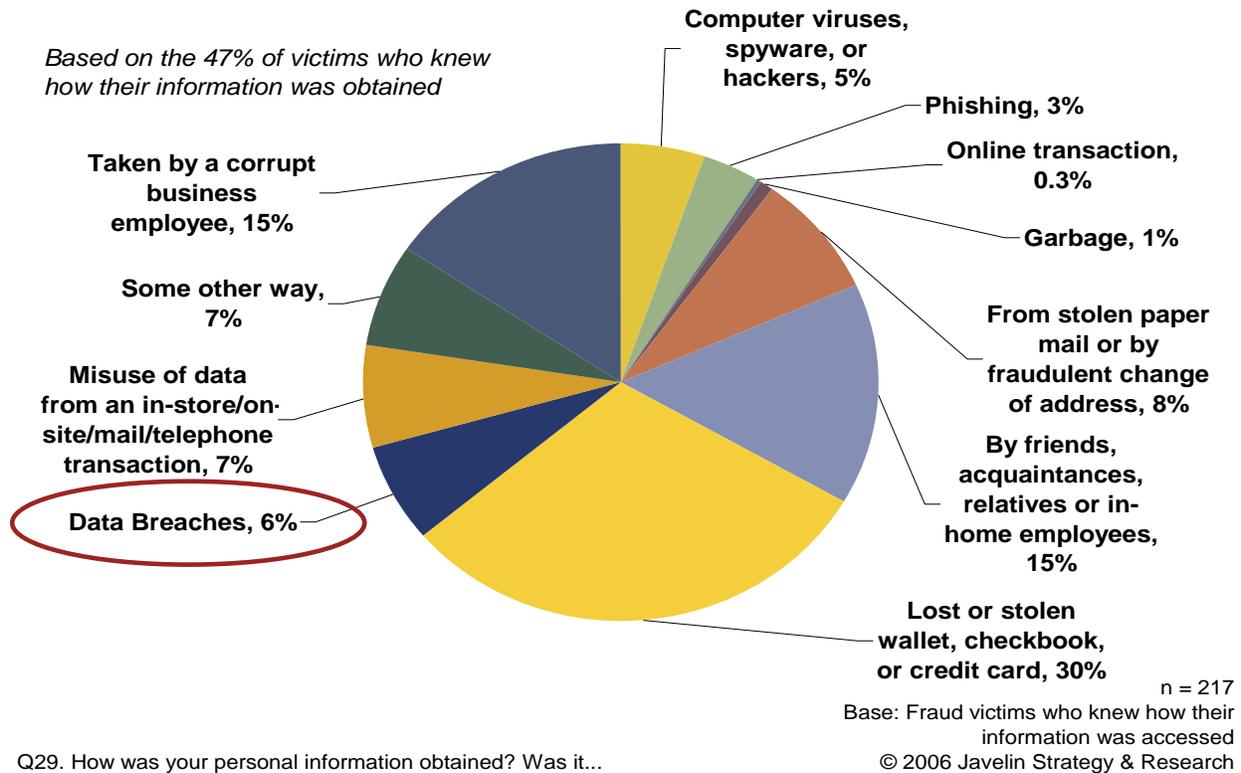
Publication date: August 2006

Subscribers to Javelin’s syndicated research service are invited to submit inquiries related to this or any other topic. Please contact us via inquiry@javelinstrategy.com.

**Data Breaches and Identity Fraud:
Misunderstanding Could Fail Consumers
and Burden Businesses**



Consumer Fears Misplaced: Data Breaches Generate Only Six Percent of ID Fraud
Other Points of Access Trigger More Exposure for Consumers



Q29. How was your personal information obtained? Was it...

Comparing the relative level of public attention data breaches receive, consumers are being misdirected in their priorities for guarding against identity fraud. Javelin data indicates that among identity fraud victims who know how their information was obtained only six percent indicate a data breach as the source.¹ By contrast, lost or stolen wallets and checkbooks are reported as sources of fraud five times more frequently at 30%. Information taken by close associates or family members is cited by 15%. It is clear that there are other areas of exposure for consumers' attention that could have a far greater payoff in risk reduction.

When data breaches do occur, the circumstances of the theft and the types of data stolen should guide the actions offered to customers, whether it be credit monitoring services, fraud alerts, security freezes,² account closure or other responses. Breaches that are targeted specifically to obtain private data are clearly more serious than breaches where the information is obtained incidentally. The specifics of when to offer credit monitoring services and the types of services to offer is beyond the scope of this report; however, financial institutions should know that there is a structured, analytic process of evaluating whether to offer credit monitoring services and the precise types of services to proffer depending upon the variables of the breach.³

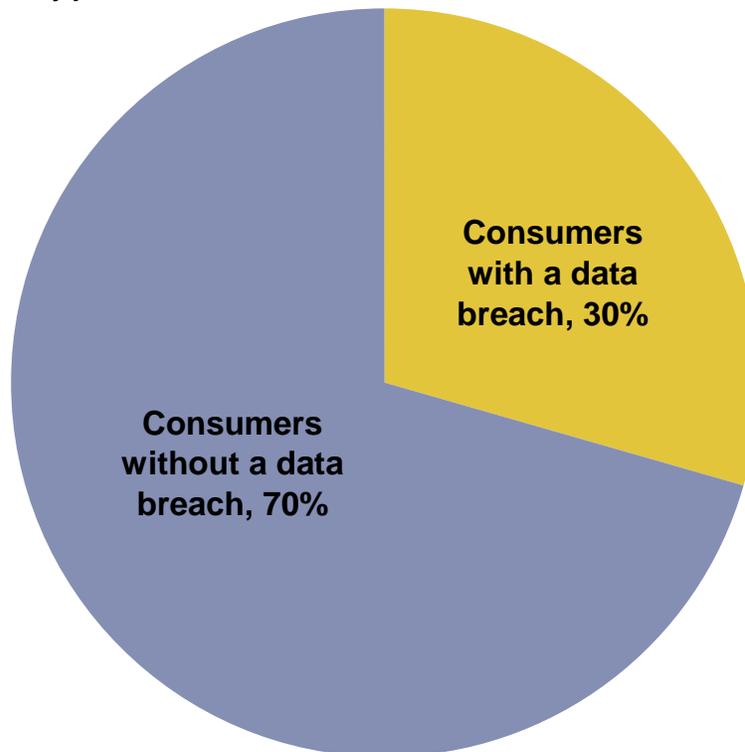
¹ **2006 Identity Fraud Survey**, Javelin Strategy & Research, 53% of ID fraud victims knew how their information was obtained.

² Ability to turn off credit reports so that new accounts which require reports cannot be opened.

³ **Credit Monitoring for Data Breaches**, Javelin Strategy & Research, Custom Consulting, 2006

Data Breaches Hit a Significantly Large Group of Consumers

Growing Notification May just Become “White Noise”



Note: Data based on reports of known data breaches in the US between Feb 2005 and Feb 2006

Base: US adults
© 2006 Javelin Strategy & Research

Three out of every ten U.S. accountholders suffered a known data breach in the last year alone. Javelin derived this figure by taking the publicly disclosed data breaches of 55 million accounts⁴ and adjusting for non-multi-state public data breaches for those states without reporting laws.⁵ Forty million of these breached accounts were accounted for by the CardSystems data breach alone.⁶ By contrast, in Javelin’s 2006 national survey of over 5,000 U.S. adults, only 1.3% report being notified of a data breach (five-year averages).⁷ Data breach notification has only recently started to become legislated—currently 28 states have differing data breach notification laws on the books and more are pending.⁸ Therefore it is reasonable to expect the percentage of respondents who were notified of a data breach to rise sharply in the next survey.

⁴ www.privacyrights.org Year starting with the ChoicePoint breach announced in Feb. 2005, ending in Feb. 2006

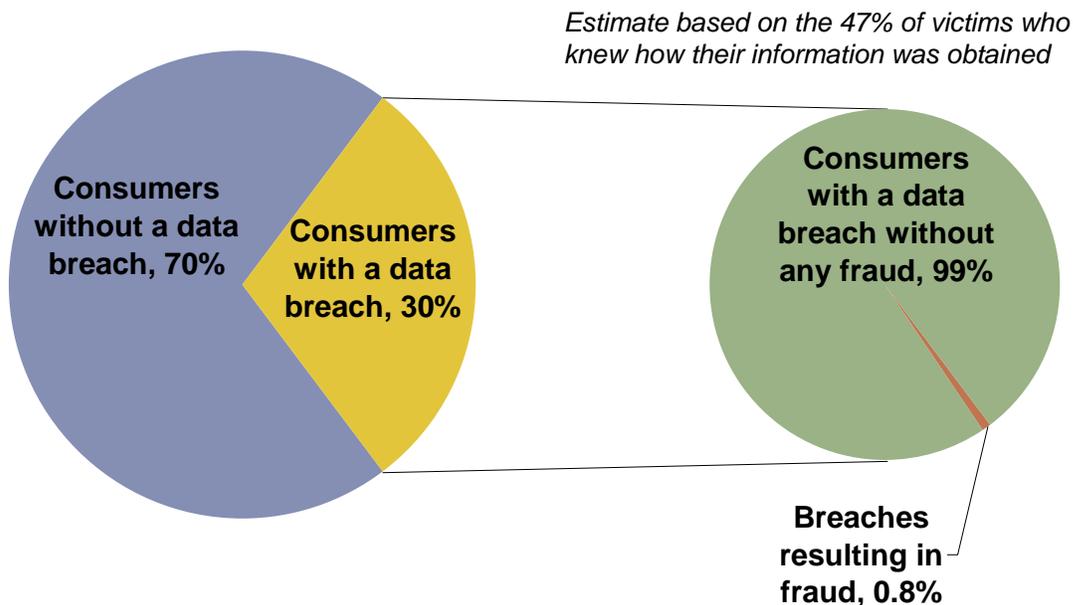
⁵ Norm-adjusted at 5.59% for non-multi-state public data breaches using CA and OH full year disclosure averages

⁶ Statistical outlier

⁷ **2006 Identity Fraud Survey**, Javelin Strategy & Research, January 2006

⁸ <http://www.ncsl.org/programs/lis/cip/priv/breach06.htm>

Media Reporting about Data Breaches is Disproportionate to Low Fraud Rates
Good News Needs Equal Air Time



Note: Data based on reports of known data breaches in the US between Feb 2005 and Feb 2006
Q29: How was your information obtained...?

n = 5,000
Base: US adults
© 2006 Javelin Strategy & Research

While the exposure, publicity and fear surrounding data breaches increased exponentially in 2006, the total dollar amount of identity fraud in the U.S. only increased four percent over the same time period. This additional information is not receiving sufficient coverage. Of those consumers with known data breaches, the percentage that suffers fraud is only 0.8%, or eight out of every 1,000. Very large breaches, while extremely serious for the organizations involved, convey inversely less risk to each individual account holder. The ChoicePoint data breach of 162,000 accounts has thus far resulted in 800 instances of fraud for a percentage of 0.5%.⁹

In 2006, the quantity of Americans who suffered from identity fraud actually declined.¹⁰ Meanwhile publicity of data breaches is widespread; leaving the clear impression that actual fraud committed by utilizing data uncovered in breaches is far more prevalent than in real life. Data breaches undermine public confidence in the violated institution and in the system as a whole. The fear that is being generated is out of proportion to the resulting fraud, which is minimal.

⁹ <http://www.ftc.gov/speeches/majoras/060223californiaidtheft.pdf> Note: It is possible this number may rise in the future.

¹⁰ **2006 Identity Fraud Survey**, Javelin Strategy & Research, 8.9 M victims in 2006, 9.3 M victims in 2005, Jan 2006

Can Consumers Be Better Protected by Less Burdensome Legislation?

A federal mandate will have sweeping consequences on corporate practices; it is imperative that the legislature fully understand the nature of the data breach problem before acting. While national legislation is needed to protect consumers and unify the myriad state laws, imposing overly strict and extensive reporting requirements regardless of risk that will last for years to come is perhaps not in the public's best interest.

California's law SB 1386—the first notification law to go into effect on July 1, 2003—requires automatic notification whenever private data has been breached—unless the data is encrypted.

Data breaches are defined as names matched with social security numbers, driver's license or state identification numbers; or account numbers or credit or debit card numbers with passwords or codes. With 28 states now having legislated differing versions of data breach notification bills and a dozen more pending, compliance is becoming more complex by the day.

Although a national plan to unify this hodgepodge of states' bills is necessary and popular with businesses and consumers alike, the reality has been more problematic, with as many as ten different bills introduced in the House and Senate to address this issue. The most likely candidate, H.R. 3997, the Financial Data Protection Act, has been opposed by certain consumer groups who regard it as weakening some states' (like California's) bills because notification is required only if there is "risk of substantial harm or inconvenience to the consumer."

The original legislation was important to alert businesses and consumers to the hazards posed by under-protected electronic data. There's no justification for organizations to indiscriminately allow employees to make thousands of individual's private records accessible through laptops, PDAs or other easily-stolen devices. Such continued breaches will send the message that organizations can't be trusted to correct lax security.

But tying businesses to strict long-term automatic reporting requirements *regardless of fraud risk* may end up generating useless white noise for consumers in the years to come. As knowledge has increased about electronic data breaches a concerted response has been made by industry to lower breach exposure and strengthen security practices, by the use of risk assessments, restricted access, encryption, and exercising tighter control over sensitive data, among other means. Additionally, technological advances such as biometrics, two-factor identification and advanced patterning software can quickly alter the financial landscape.

Federal data protection legislation is desirable to safeguard consumers and unify states' bills; but imposing strict long-term automatic notification requirements regardless of risk in the face of low actual fraud rates may not be logical in today's fast-changing environment.

Understanding is Vital to Drafting Intelligent Legislation

Federal data breach reporting legislation is necessary

- ✓ To protect all U.S. consumers
- ✓ To unify data breach processes for multi-state businesses

Misunderstanding of problem:

- ✓ Large numbers of data breaches—but very few instances of fraud

Recommendation: include "risk assessment" in new federal law

- ✓ Technology changes quickly, laws slowly
- ✓ Strict automatic reporting requirements "regardless of risk" may create white noise for consumers for years to come