

SOCIAL SECURITY

Maryland

Class C Driver's License

EXPIRES

BANKING TWENTYFOUR

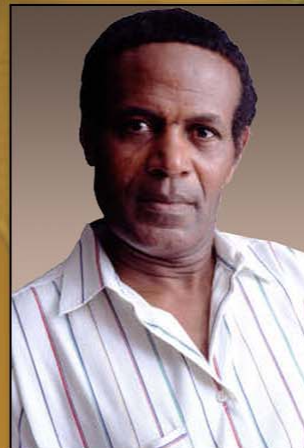
MasterCard

EUROCARD

# REPORT ON THE ATTORNEY GENERAL'S IDENTITY THEFT FORUM

MARYLAND ATTORNEY GENERAL  
J. JOSEPH CURRAN, JR.

FEBRUARY 8, 2006



**FORUM ON IDENTITY THEFT IN MARYLAND:  
PROTECTING AND HELPING MARYLAND CONSUMERS**

Report on Proceedings

November 21, 2005  
Maryland Office of the Attorney General  
200 St. Paul Place  
22<sup>nd</sup> Floor Conference Center  
Baltimore, Maryland

A forum sponsored by the Maryland Office of the Attorney General  
J. Joseph Curran, Jr.,  
Attorney General of Maryland

## **MESSAGE FROM THE ATTORNEY GENERAL**

Because of the prevalence of identity theft in Maryland and the terrible impact it has on victims, I decided to conduct an Identity Theft Forum to explore solutions to this problem. Although there are many aspects to the issue of identity theft, the focus of the forum was state legislative measures that are needed in order to ensure the privacy and security of the personal information of Maryland residents, and to help Marylanders protect themselves from identity theft. Among the topics considered in the forum were “security freeze” laws that allow consumers more control over their credit reports and security breach notification laws that provide for notification to customers when the customers’ personal data has been accessed improperly. I also asked the participants to discuss other measures that should be considered.

I applaud the Maryland General Assembly for creating an Identity Theft Task Force to study measures that can be taken to address the problem of identity theft, and my office is a member of that Task Force. However, the report of the Task Force is not due before December 31, 2006, and action on any recommendations could not take place before the General Assembly’s 2007 session. Accordingly, I convened this Forum because I believe that the growing problem of identity theft requires that Maryland take steps now to protect consumers with legislative measures that already have been tested in other states.

I invited identity theft victims, consumer advocates, privacy experts, business representatives, and legislators to participate because I wanted to hear from as many different perspectives as possible. I found the participants’ contributions very helpful, and I am issuing this report with the hope that it will help to direct attention to this important issue and to advance efforts to address this significant problem.

**J. JOSEPH CURRAN, JR.**

## TABLE OF CONTENTS

Introduction .....	1
Forum Participants .....	2
Impact of Identity Theft on Victims .....	3
Discussion of Security Freeze Legislation .....	7
Discussion of Security Breach Notification Legislation .....	12
Discussion of Other Approaches for Assisting Identity Theft Victims .....	15
Recommendations .....	17
Appendix A: Forum Agenda	
Appendix B: FTC Complaint Data, National and Maryland	
Appendix C: Data Security Breaches (2000 - 2005)	

## INTRODUCTION

When the Federal Trade Commission (FTC) began keeping specific statistics on identity theft in 2000, the number of complaints it received from identity theft victims was 31,000. Last year, that number had grown to over 250,000.<sup>1</sup> As disturbing as these numbers are, they are an underestimate of the identity theft problem since they only count complaints received by the FTC. Although estimates of the number of identity theft victims vary, one of the most thorough recent reports estimated that the number of identity theft victims last year was 9.3 million, and the amount of the thefts was \$52.6 billion.<sup>2</sup>

Over the last year, the related problem of security breaches also has become a major issue. Beginning in early 2005, the many instances of massive data security breaches have made consumers across the country aware of the importance of data security, and how a security breach can threaten the privacy of their personal information. According to the Privacy Rights Clearinghouse, these data breaches have affected as many as 50 million people.<sup>3</sup>

Although this is a national problem, identity theft is an especially significant problem here in Maryland. In the most recent FTC study, Maryland ranked 11<sup>th</sup> among the 50 states in the number of identity theft victims as a percent of its population.<sup>4</sup> Maryland consumers also have been affected by recent security breaches. In fact, 2,750 Maryland consumers were affected by just one of the breaches, when thieves improperly accessed information held by ChoicePoint, a large data broker.<sup>5</sup>

In the 2006 session, the General Assembly has the opportunity to continue its efforts to address the issue of identity theft. In the last session, several pieces of legislation were enacted that will help Maryland consumers avoid and recover from identity theft. One bill provided for greater privacy protections for Marylanders' social security numbers.<sup>6</sup> Another bill required a local law enforcement agency, after being contacted by a person who knows or reasonably suspects that the person is a victim of identity fraud, to prepare and file a report of the alleged identity fraud and provide a copy of the report to the victim.<sup>7</sup> And another bill established a task force to study problems associated with identity theft in Maryland and privacy laws in other states.<sup>8</sup> These bills represent significant progress. However, more can be done to help Marylanders. Among other topics, this forum considered two promising legislative approaches to helping consumers: (1) security freeze legislation and (2) security breach notification legislation.

## FORUM PARTICIPANTS

Forum Moderator: **J. Joseph Curran, Jr.**  
Attorney General of Maryland

**The Honorable Susan C. Lee**  
Delegate  
Maryland General Assembly

**Darrin E. Brown**  
State Director for Advocacy  
AARP Maryland Office

**The Honorable Neil F. Quinter**  
Delegate  
Maryland General Assembly

**Evan Hendricks**  
Editor, Privacy Times  
Author of *Credit Scores and Credit Reports*

**The Honorable Doyle Neimann**  
Delegate  
Maryland General Assembly

**Cheryl Hystad**  
Executive Director  
Maryland Consumer Rights Coalition

**Sharon Stone**  
Identity Theft Victim

**Chantele Mack**  
Manager for Government Relations  
Consumer Data Industry Association

**Andrea Murphy**  
Identity Theft Victim

**Ronni Burns**  
Director of Business Practices  
Citi Credit Cards  
Citigroup

**Sonya A. Smith-Valentine, Esq.**  
Valentine Legal Group, LLC

**Nicole Robinson**  
Identity Theft Resource Center

**Edward Steinberg**  
Owner  
J.S. Edwards LTD

**Edmund Mierzwinski**  
MaryPIRG  
National Consumer Advocate

**Carla Stone Witzel, Esq.**  
Counsel to the Maryland Bankers Association  
Partner, Gordon, Feinblatt, Rothman,  
Hoffberger & Hollander, LLC

**Brad Heavner**  
MaryPIRG  
State Director

In addition to the participants listed above, the following invitees who were unable to attend submitted written remarks:

**Angela Butler**  
Identity Theft Victim

**Chris Jay Hoofnagle**  
Senior Counsel  
Electronic Privacy Information Center

## **IMPACT OF IDENTITY THEFT ON VICTIMS**

### **Background**

The burden of identity theft on victims is considerable.<sup>9</sup> Dealing with the consequences of identity theft is a time-consuming and often frustrating process for victims. A study by the FTC indicated that the average victim spends 30 hours resolving problems related to identity theft.<sup>10</sup> Victims also spend an average of \$500 during the process of correcting problems caused by identity thieves.<sup>11</sup> In order to understand the real world problems that consumers face, the Attorney General invited victims of identity theft to relate their stories about their experiences. In addition, victim advocates were invited to tell about their work in helping victims recover from identity theft.

### **Participant Comments**

Maryland resident Sharon Stone began to suspect that she had been a victim of identity theft when she received a phone call in 1999 from a store asking if she had opened a credit card account. She informed the store that she knew nothing about the account. Since she was concerned by this call, she started to monitor her accounts and credit reports. Not long afterwards, she began seeing new credit that had been extended – purportedly to her – that was fraudulent. The identity thief apparently had been able to obtain her name, date of birth, and social security number, and was using the information to open new accounts. Ms. Stone contacted local police and the credit reporting agencies about this identity theft. However, she continues to see information reappear on her credit reports related to the fraudulent accounts that she thought had been removed. The total for these accounts is \$10,000 and is still growing.

Ms. Stone noted that one particularly frustrating part of her experience has been the difficulty she now has in trying to rent apartments. Since 1999, when Ms. Stone applies for apartments, she faces difficulty when the landlord runs a credit check. When the landlord reviews her credit report, it often shows the fraudulent items caused by the identity theft. As a result, most landlords reject her rental applications, and she has had a very difficult time trying to find a place to live.

Andrea Murphy spoke on behalf of her son, Andre, who discovered someone had stolen his identity. In 2002, when Andre was 18 years old, he applied for a job at the U.S. Department of Justice. During the background check, which included an examination of Andre's credit history, it was discovered that an identity thief had created \$45,000 in debts in Andre's name, including the purchase of a \$25,000 car. Ms. Murphy spent many hours and took time off from her job to look into these debts. She reported

the identity theft to local law enforcement personnel and to the credit reporting agencies. Eventually, she discovered that the identity thief was a 43-year-old Baltimore man who worked for the Social Security Administration, and who had been using Andre's name and social security number to obtain credit since Andre was 16 years old. The man was caught and prosecuted, but received only probation. As part of the case, the man was required to write a letter stating that he was the person who had used Andre's name and created the debts that appeared on Andre's credit report. However, Andre still receives letters from collection agencies related to these debts.

Another identity theft victim, Julie Butler, who was unable to attend the forum, submitted written remarks. In 2003, Ms. Butler's purse was stolen. Among the items in the purse were her driver's license and her paycheck that listed her social security number. Two weeks later, Ms. Butler received a bill for a recently-opened cellular phone account that she knew nothing about. Because of this, she obtained copies of her credit reports, which indicated there were numerous credit inquiries made by businesses related to the opening of new accounts. In the course of contacting the businesses that had made the inquiries, she discovered that, among other purchases, the identity thief had bought two new trucks in Ms. Butler's name and opened accounts in seven different Maryland counties. Although she contacted the police departments in most of these counties, the only department that was responsive was Baltimore County. Ultimately, Ms. Butler discovered that the identity thief was a 16-year-old girl who was part of a criminal gang. At one point, several members of the gang, including the girl that had posed as Ms. Butler, were apprehended on an unrelated charge. However, when the girl produced Ms. Butler's license, which had no criminal record connected with it, she was released. This girl still has Ms. Butler's information, and remains at-large.

Ms. Butler indicated several things that she found most frustrating. First, she was concerned that most of the police departments that she contacted about the theft were not responsive. Second, she had difficulties with the Motor Vehicles Administration (MVA) in connection with a fraud alert on her driver's license. Even though she had placed a fraud alert on her license, the MVA had changed Ms. Butler's address to the false address used by the identity thief when she purchased one of the trucks. Ms. Butler also received a notice of suspension of registration privileges due to the use of the false address.

Sonya Smith-Valentine, an attorney with the Valentine Legal Group whose practice includes assisting victims of identity theft, mentioned several issues that she sees regularly in her clients' cases. First, losing money is not the only threat from identity theft. Her clients often become aware of the occurrence of identity theft when they are turned down for a job or when their application to rent an apartment is rejected,

such as the case of Ms. Stone. Ms. Smith-Valentine also mentioned that one great source of frustration is dealing with fraudulent items on credit reports again and again. The appearance of previously-deleted fraudulent items is sometimes referred to as "repollution" of the credit report. She says that most of her clients do all the right things when they discover the identity theft – i.e., reporting the theft to the credit reporting companies, the police, and the companies that issued the credit. However, the items keep reappearing on the victims' credit reports.

Nicole Robinson, the regional representative of the Identity Theft Resource Center, a national nonprofit organization that helps victims of identity theft, agreed with Ms. Smith-Valentine that there is a significant problem with repollution of credit reports. She mentioned that one source of the problem is the selling of debts. Although an original creditor may be aware that a debt is connected to identity theft, when the debt is sold to another business, it may be re-reported as a bad debt by a new creditor when placed for collection. Ms. Robinson also mentioned that identity thieves cause problems for victims in more ways than just putting fraudulent items on their credit reports. Some of the impacts on victims are less obvious. For example, Ms. Robinson, who is also an identity theft victim, said that in her case, she is seeing negative information appear on her credit report that is based, not on items fraudulently purchased by her identity thief, but on her identity thief's poor credit record. Her identity thief's bad credit history is being channeled onto Ms. Robinson's credit report.

Maryland Delegate Doyle Neimann, who is an Assistant State's Attorney for Prince George's County, mentioned another problem that victims experience. When a criminal is charged, often aliases and AKAs are listed, which are entered into databases. This could cause problems for identity theft victims if one of the identity thief's AKAs is the name of the victim. If someone does a criminal record check of the victim, it might appear that the victim has a criminal record, when, in fact, the entry in the database refers to the identity thief.

Maryland Delegate Susan Lee noted that several laws have been enacted already that will help Ms. Stone and Mr. Murphy. For example, she cited recently-enacted bills in the General Assembly that assist identity theft victims in filing police reports and that clarify criminal jurisdictional issues in cases where the incidents in an identity theft case occur in more than one jurisdiction. She also mentioned changes in the federal Fair Credit Reporting Act that provide more help to identity theft victims.

Evan Hendricks, the editor of *Privacy Times* and author of *Credit Scores and Credit Reports*, called attention to the human cost of identity theft. He noted that some people ask what the cost of identity theft is to consumers when the costs are often borne

by the credit card industry or by retailers. In fact, there are costs, as is highlighted by the testimony of Ms. Stone and Ms. Murphy: not getting an apartment, not getting a job, or not getting a loan you need. This is in addition to all the time, effort, and opportunity costs spent in correcting fraudulent credit information on victims' credit histories.

Mr. Hendricks said the testimony by the victims shows that the credit report is at the epicenter of identity theft. When the identity thief tries to get new credit, the credit report enables the crime. And afterwards, the credit report becomes the main source of damage to the victim.

Darrin Brown, the State Director for Advocacy for the AARP Maryland Office, stated that seniors are disproportionately represented among identity theft victims, and AARP is trying to do as much education among its membership as it can. These efforts are especially important now because of implementation of Medicare Part D, the prescription drug benefit. There are many things that are helpful to seniors in Medicare Part D. But at the same time, the implementation provides many opportunities for identity thieves to attempt to obtain personal information from seniors. For example, identity thieves are calling seniors purportedly to assist them in enrolling in Part D, but are actually trying to obtain their names and account numbers.

## **DISCUSSION OF SECURITY FREEZE LEGISLATION**

### **Background**

Although current federal law provides some tools to help victims deal with the consequences of identity theft, they do not prevent identity fraud from occurring or recurring.<sup>12</sup> In an effort to provide consumers with a more effective tool in preventing identity theft, twelve states have enacted laws that allow consumers to place “security freezes” on their credit reports.<sup>13</sup> A major goal of a security freeze is to stop “new account fraud.” It is common for identity thieves to open new accounts using their victims’ names and information. When there is no payment on these accounts, the creditors pursue the victims, whose credit is often ruined. New account fraud costs consumers and businesses significantly more money than identity fraud on existing accounts.<sup>14</sup> In addition, victims spend more than four times longer resolving problems related to new account fraud than fraud related to existing accounts.<sup>15</sup>

A security freeze gives consumers the right to prevent credit reporting agencies from making their credit reports available to creditors for the purpose of issuing new credit. The freeze prevents access to the report, except for circumstances such as when a business reviews an existing account or when the consumer gives express permission for the release of the report. If an individual's credit file is frozen and an identity thief applies for credit in that individual's name, a creditor almost certainly would deny the application, preventing an instance of identity theft. The laws allow consumers to “unfreeze” the credit report when the consumer wants to apply for new credit.

### **Participant Comments**

Edmund Mierzwinski, a National Consumer Advocate for MaryPirg, stated that the best defense against identity theft is to control access to your own credit report. He said that most types of new account fraud would be preventable if consumers had the ability to freeze access to their credit files. Businesses will not open a new account if they can’t do a credit check on the potential borrower. The benefit of a security freeze is that it allows consumers to prevent identity theft instead of just helping consumers after they have been victimized. Mr. Mierzwinski also mentioned that PIRG recently released a new version of its model security freeze legislation.

Delegate Neil Quinter said that it should be remembered that no one is arguing that a security freeze is appropriate for everyone in all circumstances. For some consumers, a security freeze might actually cause more difficulties than it is worth. However, for at-risk consumers and some others, it would be extremely helpful.

One issue that was raised was the possibility that the security freeze process might confuse and frustrate consumers. Edward Steinberg, the owner of the clothing retail store J.S. Edwards LTD, said that he recognized that the protection provided by a security freeze would be very helpful to consumers, and would be a very good tool to avoid some types of identity fraud. However, he also indicated that many consumers probably would be confused about how a security freeze would work. For example, an unsophisticated consumer, who has a security freeze, and a salesperson might spend a significant amount of time before the consumer finally decides to purchase an item. Then, if the consumer tries to open a new account to purchase the item, both the consumer and salesperson would realize that the account could not be opened immediately. Consumers who have become accustomed to instant credit would be frustrated and the salesperson would have wasted his time.

Brad Heavner, the State Director of MaryPIRG, responded by saying that any confusion could be addressed by educating consumers about the process. He believed that consumers who wanted to take advantage of security freezes would not have difficulty unfreezing their credit files prior to applying for new credit. Nicole Robinson agreed with Mr. Heavner that the process would not cause significant difficulty since the people most likely to take advantage of the freezes would be people who think they are at-risk for identity theft, such as Andre Murphy and herself. People who consider themselves to be at-risk would likely ensure that they are familiar with the process. Ms. Robinson said that the good thing about a security freeze is that it can prevent identity thieves from going on spending sprees. In the case of Andre Murphy, and in her own identity theft case, the identity thief is not in jail. The thieves could still open new accounts. Having a security freeze would prevent that from happening. Sonya Smith-Valentine agreed, relating the case of one of her younger clients who, in the process of applying for his first car loan, discovered that someone had been using his information to obtain credit since he was six years old. Every time he checks his credit report, the thief has opened a new account. Ms. Smith-Valentine says that a security freeze would help break this cycle.

Another issue that was brought up was whether protections in federal law that are available to consumers already are sufficient to protect consumers. Chantele Mack, the Manager for Government Relations at the Consumer Data Industry Association, stated that many of the problems encountered by identity theft victims could be addressed by existing federal laws that allow victims to place fraud alerts on their credit files and block fraudulent information that appears on their reports. Educating consumers about these laws, therefore, should be a priority. Mr. Mierzwinski responded that, while existing federal laws were helpful to victims, a security freeze is the only solution for people who are not already victims. The federal rights are after-the-fact tools. They

only help after a consumer becomes a victim. A fraud alert does not prevent the potential creditor from seeing the report, and it does not prevent the credit reporting agency from selling or sharing the credit report. A freeze prevents the fraud from occurring in the first place. Andrea Murphy mentioned that fraud alerts were not sufficient in the case of her son. The identity thief in her son's case had fake identification that, apparently, allowed him to convince businesses that the thief really was Andre Murphy.

Another issue was whether consumers should have to pay a fee for freezing and unfreezing their files, and if so, what the fee should be. Chantele Mack indicated that, although she could not state with specificity how much the compliance costs would be for credit reporting companies, there would be substantial operational and start-up costs. The costs would include gearing up call centers to process consumer requests, including hiring and training staff and processing costs. She also indicated that other states that have passed security freeze legislation have allowed credit reporting companies to charge for freezing and unfreezing, such as California, which allows a charge of \$10 for freezing and \$10 - \$12 for unfreezing.

In connection with the costs of the security freeze, Edmund Mierzwinski mentioned that, in the debate over security freeze legislation in California, the credit reporting industry claimed that consumers should be charged \$50. However, if credit reporting companies sell credit reports to their clients for 30 to 50 cents each, he said, it is hard to explain why credit freezing and unfreezing should cost consumers so much. He considers the charges allowed in some states to be price gouging. He recommended that, if there is any charge at all allowed, the ceiling should be \$5. He also reminded the forum that a charge of \$5 per freeze really meant \$15 for the consumer since the consumer would have to pay all three credit reporting agencies. Brad Heavner stated that, with modern technology, much of the freezing and unfreezing process could be automated, reducing many processing costs to virtually nothing. And so, he said, we should not be talking about \$10 to freeze and unfreeze, but rather \$1.

The timeframe required for freezing and unfreezing also was brought up as an issue. Chantele Mack indicated that, in general, states that have enacted freeze laws have allowed credit reporting agencies five days to freeze a file and 3 days to unfreeze. She stated that it would be very difficult to reduce the time necessary to freeze and unfreeze a consumers' credit file. In addition to the technological challenges to freezing and unfreezing quickly, the credit reporting agencies must have sufficient time to verify that they are freezing or "thawing" a report for the correct person and are providing it (or denying it) to the correct person. If the agencies don't undertake this verification, there

is a risk of exacerbating an already-existing fraud or in compromising the security of a consumer's credit data.

Brad Heavner noted that, in modern banking transactions, you can transfer your life savings from one account to another in five minutes. With this type of technology, which can be used in unfreezing credit reports, three days is far too long to allow. Unfreezing should be a matter of minutes, not days. Edmund Mierzwinski added that a good model to follow would be New Jersey's legislation that directs credit reporting agencies to reduce the time to unfreeze a credit report to 15 minutes. He also noted that PIRG's new model security freeze legislation, like New Jersey's law, requires credit reporting agencies to reduce the time to unfreeze accounts down to 15 minutes. Edward Steinberg also commented that if unfreezing the credit report could be done quickly, that would eliminate the problems that consumers and retailers might encounter in everyday shopping situations.

Chantele Mack mentioned a problem that she saw with the effectiveness of security freeze laws. She said that a freeze might not be effective in many instances. In half of identity theft cases, the victim knows the thief. If the thief is close to the victim, and was able to steal the victim's information in the first place, then the thief would be able to obtain the victim's security freeze PIN as well, which would allow the thief to lift any freeze that the victim had placed on his or her report. Brad Heavner responded by noting that, unlike other personal data, the PIN's use would be very limited; and therefore, it is less likely that a thief could obtain the PIN easily. He also mentioned that only one in four identity theft victims know who stole their information, so it is inaccurate to say that half of identity theft victims know the thief. Delegate Quinter agreed that even if friends and acquaintances commit a significant percentage of identity theft, that doesn't undermine the utility of security freezes. Consumers can take steps to safeguard PINs.

Ms. Mack commented that we do not know the number of consumers who have taken advantage of the security freezes in states that had enacted freeze laws. She said that the industry does not keep track of these numbers. However, she was aware that, as of September 2003, approximately 5,000 consumers in California had requested freezes.

Chris Hoofnagle, the Senior Counsel at the Electronic Privacy Information Center, in submitted remarks, stated that security freezes would help to address the lax practices that the credit industry uses in extending credit, which make it easy for even unsophisticated criminals to gain access to new accounts in others' names. Because it is too easy for impostors to open new accounts in victims' names, and because existing federal protections are ineffective in preventing identity theft, legislation should

empower consumers to limit credit report availability. For a credit freeze to work, it has to be easy for consumers to use. All individuals should be able to trigger a freeze, not just identity theft victims. There should also be a method for the individual to quickly thaw their report, so that individuals can take advantage of credit and employment opportunities. Mr. Hoofnagle added that a security freeze system also solves a long-standing problem with authorized access to credit reports, the "impermissible pull." This occurs where someone with access to the consumer reporting system obtains a report on a consumer without a credit application or existing relationship with the consumer.

## **DISCUSSION OF SECURITY BREACH NOTIFICATION LEGISLATION**

### **Background**

The public has become aware of the numerous incidences of security breaches over the past year as a result of California's security breach notification law, which went into effect on July 1, 2003.<sup>16</sup> This law requires businesses to notify the public about breaches of the security of their computer information systems where personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In response to the many security breaches during 2005, twenty-two additional states have enacted security breach notification laws.<sup>17</sup>

The first security breach that received widespread attention occurred in February 2005. A security breach at ChoicePoint, a company that provides consumer information to businesses, allowed identity thieves to access the personal financial information of at least 145,000 consumers, including 2,750 Maryland residents. Since then, the public has learned of many other major data breaches. These data breaches have affected as many as 50 million people.<sup>18</sup>

Information compiled by the Congressional Research Service, which is attached to this report as Appendix C, shows that the breaches occurred in many settings, including breaches at data brokerage businesses, financial institutions, retail companies, educational institutions, and media companies. The ways in which the data breaches occurred varied, but they included computer hacking, stolen laptop computers, stolen and lost computer data tapes, and dishonest insiders obtaining information. As a result, the consumers who were affected have been placed at increased risk of identity theft, fraud, and other crimes.

### **Participant Comments**

Edmund Mierzwinski said that there are two real issues for security breach legislation. The first issue is when will businesses be required to provide notice. He said that businesses should always be required to provide notice when there has been a breach. Breach legislation should not allow businesses to decide that notice is not required because the breach creates no material risk to consumers. If this type of "risk trigger" is allowed, consumers will not be protected. Since businesses themselves will be in charge of deciding when they have to send out notifications, breach legislation will not provide an additional incentive to improve security of consumer data. And in fact, most of the states that have enacted security breach legislation have not included a risk trigger.

The second issue, Mr. Mierzwinski noted, is who will be exempted from the law. He said that banks are pushing hard to be exempted from security breach legislation, because they are regulated by federal law. However, under the federal Gramm-Leach-Bliley Act, states have the right to pass privacy laws stronger than federal standards. States should pass stronger legislation in the area of security breach notification because federal rules related to banks provide for a risk trigger, and consequently, are too weak to be helpful.

Carla Witzel, the legal counsel to the Maryland Bankers Association, responded that banks should be treated differently than other businesses because they are already subject to strong and broad federal laws to provide notice in the event of a security breach. Almost every state that has passed a security breach law has accorded special treatment to financial institutions in light of federal regulations. Most have said that compliance with federal law is deemed to be compliance with state law. Ms. Witzel said that, under federal rules, there is some judgment involved, so not every breach is subject to notification. This is because not all breaches create risks for consumers. In addition, she added, state laws that regulate financial institutions in this area subject these institutions to layer upon layer of different requirements in the data breach area. This is inefficient and unnecessary because the federal regulations provide consumer protections.

Mr. Mierzwinski responded by stating that financial institutions can comply with both state and federal law by complying with the strictest law. Since the current federal standard is weak, states should set the bar for notification higher.

Evan Hendricks said that many businesses are arguing that if there is no risk trigger in security breach laws, then businesses will be forced to send out notices even in the case of trivial breaches. However, there is no evidence that this is a problem. According to the FTC, there have been approximately 120 notices that have been sent out under state laws. He is unaware of even one case of a trivial notice. Further, Mr. Hendricks said, he does not know of anyone complaining about receiving a trivial notice. Mr. Hendricks added that he believes that businesses' concerns about providing too much information to consumers in this case is somewhat disingenuous. The same businesses rarely express concern about putting too much information in consumers' mailboxes when offering credit.

Mr. Hendricks also stated that the content of the notices is an important issue. The notices should provide as much information for the affected consumers as possible. This will allow consumers to make informed judgments about what actions they need to take.

Darrin Brown stated that state law has an important preventative role to play in the security breach area. The public would not have known about the ChoicePoint data breach if it were not for the California law. When someone's personal information has been compromised, they have a right to know about it. A notification law would be helpful to seniors. Seniors tend to read and act on notifications more than the population in general. If they receive notice, they will be able to take steps to reduce their risk.

Ronni Burns, the Director of Business Practices at Citigroup Citi Credit Cards, said that there were both benefits and drawbacks to security breach notification laws. But in any case, the real issue is education. Even when consumers receive notices, the first question they ask is "now what do I do?" Both businesses and government should work to inform consumers on how they can avoid identity theft.

## **DISCUSSION OF OTHER APPROACHES FOR ASSISTING IDENTITY THEFT VICTIMS**

### **Background**

The primary focus of the forum was discussion of security freeze and security breach legislation. However, an opportunity was provided to the Participants to discuss other approaches and proposals to address identity theft.

### **Participant Comments**

Evan Hendricks suggested three areas that should be considered seriously. First, he said the issue of the protection of consumers' social security numbers is critical. Too many businesses demand social security numbers in transactions in which there is no need for them, which places consumers at risk. He recommended the model language developed by PIRG for the protection of social security numbers. Second, consumers should have access to their own information that is held by businesses. Although under current law, consumers have access to their credit reports, they often are unable to obtain their information from data brokers. Consumers should have the right to access this information that is in the hands of data brokers. Third, states should consider following the example of California which has created an Office of Privacy Protection. This would help because there would be a single point-of-contact for consumers with concerns about protection of privacy.

Ronni Burns stated that regardless of new legislation, the first line of defense in the area of identity theft is the consumer. Therefore, consumer education should be the first priority. Businesses can help, as many do already. She provided the example of Citicard, which notifies consumers when there is a pattern of credit card activity that might indicate fraud. She also mentioned that Citicard has an initiative that provides comprehensive consumer education through its website that is available to anyone, and has a facility based in Maryland that specifically helps its customers who are dealing with identity theft.

Ms. Burns also said that greater attention should be given to the prosecution of identity thieves. She mentioned that Citigroup has many field investigators with expertise in investigating identity theft. There is an opportunity for greater cooperation between industry and state enforcement officials in information-sharing and prosecution.

Carla Witzel agreed that prosecution of identity thieves should be a priority. Consumers, businesses, and government all have a shared interest in bringing thieves to justice.

Delegate Doyle Neimann agreed that there is a shared interest, but commented that, for a variety of reasons, identity theft cases are very difficult to prosecute. Prevention should be as important, if not more so, than prosecution. In light of this, he said, measures such as security freezes and security breach notifications, as preventative tools, make sense.

Sonya Smith-Valentine recommended greater regulation of mail solicitations and pre-approved offers. She has clients who became victims because identity thieves intercepted the clients' mail, which had the clients' account numbers and other information. The thieves were able to access accounts or respond to offers based on this intercepted information.

Chantele Mack mentioned that one topic that has been considered is greater regulation of businesses' security standards. She indicated that, in the case of the credit data industry, there is strong regulation already. And further, because of the importance of reputation, business have a strong incentive to provide security already.

Angela Butler stated, in written remarks, that it would be very helpful if the police could see fraud alerts that had been placed on MVA records when they search drivers license data. If police had this ability, they would have apprehended her daughter's identity thief when the thief had been stopped on an unrelated charge and used her daughter's drivers license.

Chris Hoofnagle, in submitted remarks, stated that security freezes should be supplemented by additional protections against irresponsible credit granting. For instance, credit grantors should have to screen customers more carefully. California has enacted a law that requires an instant credit grantor to match identifiers from the application to the credit "header" on file at the credit reporting agency. Although the California requirement is imperfect, it could be strengthened to require the matching of more identifiers, which would make identity theft much more difficult to commit. Mr. Hoofnagle also stated that credit grantors should be liable for damages when negligent in issuing a new account to an impostor.

## RECOMMENDATIONS

Based on information gathered at this Forum and on other research and investigation, and for the purpose of improving the security and privacy of the personal information of Maryland residents, the Office of the Attorney General makes the following recommendations.<sup>1</sup>

- Maryland should enact a security freeze law that will provide Marylanders with more control over access to their credit reports. A security freeze law would benefit consumers in general, but it would be especially helpful for identity theft victims. It also would be an important supplement to existing consumer rights under state and federal law. Fees charged for the placement or lifting of a security freeze should be kept to a minimum so that this cost will not create a disincentive to the use of security freezes. In addition, both consumers and retailers would benefit from reducing the time required to lift a security freeze.
- Maryland should enact a security breach notification law. Marylanders have a right to know when their personal information has been compromised. This law should ensure that when unauthorized persons obtain access to consumers' personal information, those consumers are made aware of the situation. The notices that are provided pursuant to this law should be sufficiently detailed to allow consumers to assess their risk and take appropriate steps to minimize the risk.
- The General Assembly and the Identity Theft Task Force should give consideration to the suggestions offered by the Forum participants that are listed in the section of this report entitled "Discussion of Other Approaches For Assisting Identity Theft Victims."

---

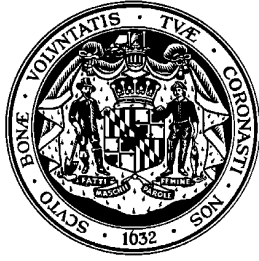
<sup>1</sup> These recommendations are solely those of the Office of the Attorney General and do not necessarily reflect the views of the Forum participants.

## Endnotes

1. *Consumer Fraud and Identity Theft Complaint Data: January - December 2005* (Federal Trade Commission, January 2006); *National and State Trends in Fraud and Identity Theft: January - December 2004* (Federal Trade Commission, 2005). Information from the Federal Trade Commission's Identity Theft Data Clearinghouse is available at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).
2. *2005 Identity Fraud Survey Report*, Javelin Strategy and Research and the Better Business Bureau (2005) available at [www.javelinstrategy.com](http://www.javelinstrategy.com).
3. Listings of, and information regarding, major data breaches are available at Privacy Rights Clearinghouse ([www.privacyrights.org](http://www.privacyrights.org)) and the Identity Theft Resource Center ([www.idtheftcenter.org](http://www.idtheftcenter.org)).
4. The FTC received 4,848 complaints from Marylanders in 2005. *Consumer Fraud and Identity Theft Complaint Data: January - December 2005* (Federal Trade Commission, January 2006); *Identity Theft Victim Complaints Trends by State, January 1-December 31, 2004* (February 1, 2005).
5. Eileen Ambrose, *Huge Theft of Identity Data Could Have Victims in Maryland: Choicepoint Sold IDs to Phony Businesses*, Baltimore Sun, February 22, 2005.
6. 2005 Md. Laws Chapter 521 (H.B. 56).
7. 2005 Md. Laws Chapter 579 (H.B. 800).
8. 2005 Md. Laws Chapter 241 (H.B. 818).
9. For detailed information on the impact of identity theft on victims, see Identity Theft Resource Center, *Identity Theft: The Aftermath 2004* (September 2005), available at [www.idtheftcenter.org](http://www.idtheftcenter.org).
10. *Identity Theft Survey Report*, Federal Trade Commission (2003), pp. 6 -7.
11. See endnote 10 above.
12. Under the Fair Credit Reporting Act (FCRA), consumers have the right to place a "fraud alert" on their credit reports. 15 U.S.C.A. §1681c-1 (1998 and Supp. 2005). When a fraud alert is placed on a consumer's credit file, creditors must take steps to verify a credit applicant's identity before extending credit. The FCRA also allows identity theft victims to block the reporting of specific information in their credit reports that is the result of identity theft. 15 U.S.C.A. §1681c-2 (1998 and Supp. 2005). However, fraud alerts and blocking only allow victims to respond to fraud after it occurs.

13. California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont, and Washington. Information on state security freeze legislation and laws can be found on the National Conference of State Legislatures' website ([www.ncsl.org/programs/banking/SecurityFreeze\\_2005.htm](http://www.ncsl.org/programs/banking/SecurityFreeze_2005.htm)) and at the Public Interest Research Group's website ([www.pirg.org/consumer/credit/statelaws.htm](http://www.pirg.org/consumer/credit/statelaws.htm)).
14. New account fraud costs victims an average of \$1,180 and businesses an average of \$10,200 per victim. The same statistics for existing accounts are \$160 and \$2,100. *Identity Theft Survey Report*, Federal Trade Commission (2003), p. 6 - 7.
15. Resolving problems related to new account fraud takes victims an average of 60 hours. Resolving problems related to existing account fraud takes victims an average of 15 hours. *Identity Theft Survey Report*, Federal Trade Commission (2003), p. 6 - 7.
16. Cal. Civ. Code § 1798.82 (2003).
17. Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, and Washington. Information on state security breach legislation and laws can be found on the National Conference of State Legislatures' website ([www.ncsl.org/programs/lis/cip/priv/breach.htm](http://www.ncsl.org/programs/lis/cip/priv/breach.htm)), and at the Public Interest Research Group's website ([www.pirg.org/consumer/credit/statelaws.htm](http://www.pirg.org/consumer/credit/statelaws.htm)).
18. *See* endnote 3 above.

**Appendix A:**  
**Forum Agenda**



**STATE OF MARYLAND**  
**OFFICE OF THE ATTORNEY GENERAL**  
*J. Joseph Curran, Jr.*

---

**IDENTITY THEFT FORUM**

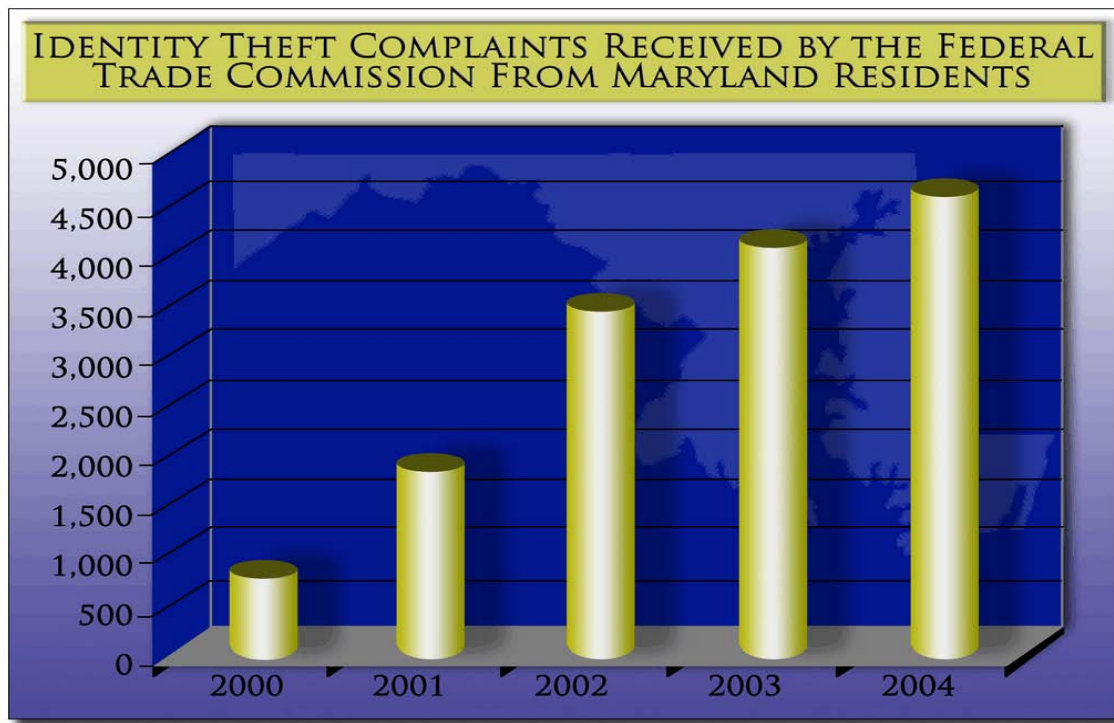
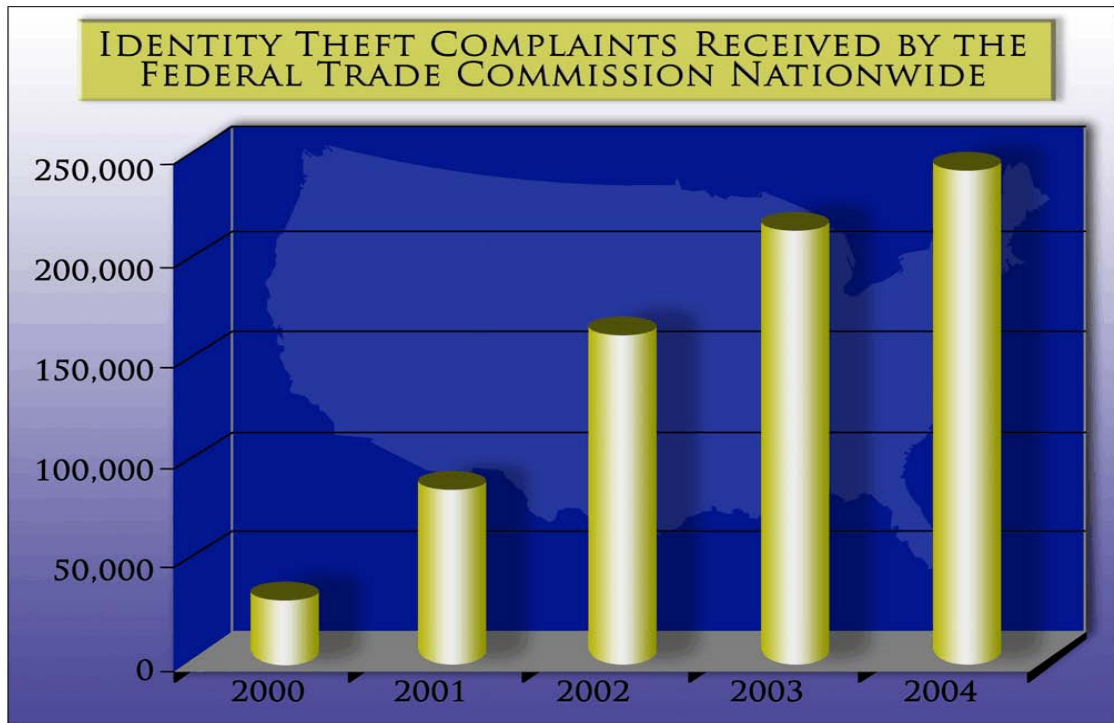
November 21, 2005  
200 St. Paul Place  
22<sup>nd</sup> Floor Conference Center  
Baltimore, Maryland

---

- 10:00 a.m. Welcome and Opening Remarks of Attorney General J. Joseph Curran
- 10:10 a.m. Impact of Identity Theft on Victims
- Identity Theft Victims' Statements
  - Discussion of Challenges Faced by Identity Theft Victims
- 10:40 a.m. Roundtable Discussion of Security Freeze Legislation
- 11:10 a.m. Roundtable Discussion of Security Breach Notification Legislation
- 11:35 a.m. Roundtable Discussion of Other Approaches for Assisting Identity Theft Victims
- Noon Closing Remarks

**Appendix B:**  
**FTC Identity Theft Complaint Data –**  
**National and Maryland**

## INCREASES IN IDENTITY THEFT COMPLAINTS TO THE FTC



## **Appendix C:**

Data Security Breaches (2000 - 2005),  
excerpted from “Personal Data Security Breaches:  
Context and Incident Summaries,” Congressional  
Research Service, December 16, 2005.

Table 1. Examples of Data Security Breaches (2000-2005)

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Sources
Boeing - theft of company computer	November 2005	current and former Boeing workers	161,000	names, Social Security numbers (SSNs), some birth dates and banking information for employees who elected to use direct deposit of payroll	Bowenmaster, David and Dominic Gates and Melissa Allison, "161,000 Workers' Personal Data on PC Stolen from Boeing," <i>Seattle Times</i> , November 19, 2005, p. A1.
Georgia Institute of Technology Office of Enrollment Services - computer theft	November 2005	past, present, and prospective students	13,000	SSNs, birthdates, names, addresses	Kantor, Arcady, "Georgia Tech Computer Theft Compromises Student Data," <i>The Technique</i> (via University Wire), November 11, 2005 at <a href="http://www.nique.net/issues/2005-11-11/news/31">http://www.nique.net/issues/2005-11-11/news/31</a> .
TransUnion (credit reporting bureau) - stolen desktop computer	November 2005	customers	3,600	SSNs and personal credit information	"Credit Bureau Burglary Leaves 3,600 Vulnerable," <i>Atlanta Journal and Constitution</i> , November 11, 2005.
Safeway - company laptop stolen from manager's home	November 2005	employees	1,200	names, SSNs, hire dates and work locations	Akkaad, Dania, "Safeway Discloses Security Breach," <i>Monterey County Herald</i> , November 5, 2005.

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Indiana University - malicious software programs installed on business instructor's computer	November 2005	Kelly School of Business students enrolled in introductory business course between 2001-2005	5,300	personal student information	"IU Finds 'Malicious' Software," Associated Press, <i>FortHwayne.com</i> , November 18, 2005, at [http://www.fortwayne.com/mld/fortwayne/news/local/13202338.htm].
University of Tennessee Medical Center - laptop computer stolen	November 2005	patients who received treatment in 2003	3,800	names and SSNs	"UT Patients Warned of Stolen Computer," <i>Chattanooga Times Free-Press</i> , November 2, 2005, p. B2.
University of Tennessee - inadvertent posting of names and Social Security numbers to Internet listserv	October 2005	students and employees	1,900	names and SSNs	"State Briefs: UT Students' Private Data Posted on the 'Net,'" <i>The Tennessean.com</i> , October 29, 2005, at [http://tennessean.com/apps/pbcs.dll/article?AID=/20051029/NEWS01/510290327/1006/NEWS01].
Bank of America - stolen laptop	September 2005	Visa Buxx card users	undisclosed	names, credit card numbers, bank account numbers, routing transit numbers	McMillan, Robert, "Bank of America Notifying Customers After Laptop Theft," <i>Computerworld</i> , October 7, 2005, at [http://www.computerworld.com/security/topics/security/story/0,10801,105246,00.html].

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Georgia - hacker hits employee records server	September 2005	current and former employees of university's College of Agricultural and Environmental Sciences	1,600	SSNs	Simmons, Kelly, "Hackers Breach Database at UGA," <i>The Atlanta Journal - Constitution</i> , September 29, 2005, p. C2.
Children's Health Council, San Jose, California - stolen backup tape	September 2005	patients, employees, and parents of patients	5,000-6,000	psychiatric records, evaluations and SSNs; also payroll data on hundreds of current and former employees and credit card information from parents of patients	Walsh, Diana, "Data Stolen from Children's Psychiatric Center," <i>San Francisco Chronicle</i> , September 20, 2005, p. B8.
Choicepoint - Miami-Dade County Police Department may have misused the department's account to illegally access consumer records	September 2005	consumers	5,103	SSNs, driver's license information	Husted, Bill, "Another Breach of Records Feared; Choicepoint Tells 5,103 Customers about Incident," <i>Atlanta Journal-Constitution</i> , September 17, 2005, p. 1H.
Miami University (Ohio) - report containing SSNs and grades of more than 20,000 students has been accessible via the Internet since 2002	September 2005	students	21,762	SSNs, grades	Giordano, Joe, "Miami University, Ohio, Finds Huge Online Security Breach," <i>Journal-News (Hamilton, OH)</i> , September 16, 2005.

CRS-8

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Kent State University - five desktop computers stolen from campus	September 2005	students and professors	100,000	names, SSNs, grades	Gonzalez, Jennifer, "Student, Faculty Data on Stolen Computers," <i>Plain Dealer (Cleveland)</i> , September 10, 2005, p. B1.
California State University - Office of the Chancellor may have experienced unauthorized access to one of its computers	August 2005	students who receive financial aid and two administrators	154	names, SSNs	"California State University Chancellor's Office Experiences Potential Computer Security Breach," <i>U.S. Fed News</i> , August 29, 2005.
J.P. Morgan (Dallas) - stolen laptop	August 2005	clients	unknown	personal and financial information	"Security Breach at J.P. Morgan Private Bank," <i>AFX International Focus</i> , August 30, 2005.
University of Florida Health Sciences Center/CharOne - stolen laptop	August 2005	patients and physicians	3,851	names, SSNs, dates of birth, medical records	Chun, Diane, "3,851 Patients at Risk of ID Theft," <i>Gainesville.com</i> , August 27, 2005 at <a href="http://www.gainesville.com/apps/pbcs.dll/article?AID=/20050827/L0CAL/208270336/1078/news1">http://www.gainesville.com/apps/pbcs.dll/article?AID=/20050827/L0CAL/208270336/1078/news1</a> .
U.S. Air Force - records stolen from the Air Force Personnel Center's online Assignment Management System	August 2005	officers and 19 NCOs	33,300	SSNs, birthdates, and other sensitive information	Dorsett, Amy, "Identity theft Threat Hangs over AF Officers," <i>San Antonio Express-News</i> , August 24, 2005, p. 1A.

CRS-9

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Colorado - hackers tapped into a database in the registrar's office	August 2005	student records from June 1999 to May 2001 and from fall 2003 to summer 2005.	49,000	names, SSNs, addresses, phone numbers	McCrimmon, Katie Kerwin, "Hackers Tap CU Registrar's Database; Privacy of 49,000 Students Potentially Invaded in Breach," <i>Rocky Mountain News</i> (Denver), August 20, 2005, p. 20A.
California State University, Stanislaus - hacking	August 2005	student workers	900	names, SSNs	Tognerti, Chris, "Hacker Breaks into Stan State Computer," <i>Modesto Bee</i> , August 16, 2005, p. B1.
University of North Texas - hacking	August 2005	current former and prospective students	38,607	names, addresses, telephone numbers, SSNs, student identification numbers, student ID passwords, student classification information and possibly 524 credit card numbers	Tessyman, Neal, "Hackers Steal Student Info from U. North Texas," <i>University Wire</i> , August 11, 2005.
Sonoma State University - hacking	August 2005	people who either attended, applied, graduated or worked at the school from 1995 to 2002	61,709	names, SSNs	Park, Rohbert, "Hackers Hit College Computer System: Identity Theft Fears at Sonoma State," <i>San Francisco Chronicle</i> , August 9, 2005, p. B2.
University of Colorado - hacking into campus Card Office (creates IDs for staff and students)	August 2005	students and faculty	36,000	university accounts and personal information	Uhs, Anna, "U. Colorado students getting (re)carded," <i>University Wire/Colorado Daily</i> , August 4, 2005.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
California Polytechnic, Pomona - two computers hacked	July 2005	university applicants and current and former faculty, staff and students	31,077	names, SSNs	Ruiz, Kenneth, "Hackers Infiltrate Cal Poly," <i>Whittier Daily News (CA)</i> , August 5, 2005.
California State University Dominguez Hills - hacking	July 2005	students	9613	names, SSNs	"Hackers crack computers, access private student information," Associated Press, July 29, 2005.
San Diego County Employees Retirement Association - hackers broke into two computers	July 2005	current and retired county government employees	33,000	workers' names, Social Security numbers, addresses and dates of birth	Chacon, Daniel, "Hackers Breach County's Personal Records: 33,000 People at Risk in Retirement Association," <i>San Diego Union-Tribune</i> , July 30, 2005, p. B1.
University of Colorado, Boulder - hackers broke into a computer server containing information used to issue identification cards	July 2005	students and professors	29,000 students and 7,000 professors	SSNs, names, photographs	"Hackers Break into CU Computers Containing 36k Records," Associated Press, August 1, 2005.
University of Southern California - individual hacked into USC's online application system	July 2005	applicants	270,000	name, address, SSNs, e-mail address, phone number, date of birth, login information	Hawkins, Stephanie, "Hacker Hits Application System at USC," <i>University Wire/Daily Trojan</i> , August 18, 2005.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Michigan State University - breach of a server in the College of Education	July 2005	students	27,000	names, addresses, SSNs, course information, personal identification numbers	"Students Informed Social Security Numbers Possibly Compromised," Associated Press, July 7, 2005.
University of California, San Diego - hackers broke into university server	July 2005	students, staff, faculty who had attended or worked at UCSD Extension in the past five years	3,300	SSNs, driver license and credit card numbers	"SD UCSD Hackers," <i>City News Service</i> , July 1, 2005.
Ohio State University Medical Center - two stolen laptops	June 2005	patients	15,000	patient names, admission and discharge dates, whether the patient had insurance, total charges and adjustments to the account.	Crane, Misti, "Laptop Containing Patients' Billing Information Stolen; Birth Dates, Social Security Numbers Not in Data Taken from Consultant, Osu Says," <i>Columbus Dispatch (OH)</i> , June 30, 2005, p. 4C.
Bank of America - laptop stolen from car in Walnut Creek	June 2005	California customers	18,000	names, addresses, SSNs,	Lazarus, David, "Breaches in Security Require New Laws," <i>San Francisco Chronicle</i> , June 29, 2005, p. C1.
Lucas County (OH) Children Services - information from the agency's personnel database was compiled and e-mailed to an outside computer	June 2005	agency's 400 current employees and about 500 others who have worked there since 1991	900	names, telephone numbers, SSNs	Patch, David, "Lucas County Children Services Data Stolen," <i>Toledo Blade</i> , June 28, 2005, p. B1.

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Connecticut - hacking - rootkit (collection of programs that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network) placed on server on October 26, 2003, but not detected until July 20, 2005	June 2005	students, staff, and faculty	72,000	names, SSNs, dates of birth, phone numbers and addresses	Naraine, Ryan, "UConn Finds Rootkit in Hacked Server," <i>eWeek</i> , June 27, 2005, at [http://www.eweek.com/article2/0,1759,1831892,00.aspx].
Eastman Kodak - laptop stolen from a consultant's locked car trunk.	June 2005	former Eastman Kodak workers	5,800	names, Social Security numbers, birth dates and benefits information	Davis, Joy, "Kodak Warns of Data Theft," <i>Rochester Democrat and Chronicle (New York)</i> , June 22, 2005, p. 8D.
University of Hawaii - dishonest library worker indicted on federal charges of bank fraud related to identity theft	June 2005	students, faculty, staff and library patrons at any of the 10 campuses between 1999 and 2003	150,000	SSNs, addresses and phone numbers	"UH Warns of Possible Identity Theft," Associated Press, June 19, 2005.
Kent State University - laptop stolen from employee's car	June 2005	full-time faculty members since 2001	1,400	names, SSNs	Hampp, David, "Kent State U. Faculty Affected by Stolen Computer," <i>Daily Kent Stater</i> (via University Wire), June 22, 2005.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
<p>Japanese credit cardholders - hackers behind U.S. data theft may have compromised the data of Japanese cardholders, according to the government. Fraudulent transactions have now emerged in Japan.</p>	<p>June 2005</p>	<p>customers of 26 domestic Japanese credit card firms</p>	<p>unknown</p>	<p>unknown</p>	<p>"Japan Cardholders 'Hit' by Theft," <i>BBC News</i>, June 21, 2005 at <a href="http://news.bbc.co.uk/2/hi/business/4114252.stm">http://news.bbc.co.uk/2/hi/business/4114252.stm</a>].</p>
<p>MasterCard - breach occurred late last year at a processing center in Tucson operated by CardSystems Solutions; one of several companies that handle transfers of payment between the bank of a credit card-using consumer and the bank of the merchant where a purchase was made. CardSystems' computers were breached by malicious code that allowed access to customer data.</p>	<p>June 2005</p>	<p>MasterCard credit card and some debit card customers</p>	<p>40 million</p>	<p>names, account numbers, security codes, expiration dates</p>	<p>Krim, Jonathan and Michael Barbaro, "40 Million Credit Card Numbers Hacked: Data Breached at Processing Center," <i>Washington Post</i>, June 18, 2005, p. A1;                      Zeller, Tom and Eric Dash, "MasterCard Says 40 Million Files Put at Risk," <i>New York Times</i>, June 18, 2005, p. A1; and                      Evers, Joris, "Credit Card Suit Now Seeks Damages," <i>CNET News.com</i>, July 7, 2005, at <a href="http://news.com.com/Credit+card+suit+now+seeks+damages/2100-7350_3-5777818.html">http://news.com.com/Credit+card+suit+now+seeks+damages/2100-7350_3-5777818.html</a>].</p>

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Federal Deposit Insurance Corporation - computer breach in early 2004. The agency wrote to employees that it learned of the breach only "recently", but did not explain how the breach occurred, aside from stating that it was not the result of a computer security failure.	June 2005	FDIC current and former employees or anyone employed at the agency as of July 2002.	6,000	names, birth dates, SSNs, and salary information	Krim, Jonathan, "FDIC Alerts Employees of Data Breach", <i>Washington Post</i> , June 16 2005, p. D1.
Motorola - Thieves broke into the offices of Affiliated Computer Services (ACS), a provider of human resources services, and stole two computers	June 2005	Motorola employees	34,000 in U.S.	SSNs and personal information	"Two Computers Stolen with Motorola Staff Data," Reuters, June 10, 2005.
Citigroup - a box of computer tapes with account information for 3.9 million customers was lost in shipment by Citifinancial, a unit of Citigroup	June 2005	personal and home equity loan customers	3.9 million	names, addresses, SSNs and loan-account data	Krim, Jonathan, "Customer Data Lost, Citigroup Unit Says: 3.9 Million Affected As Firms' Security Lapses Add Up," <i>Washington Post</i> , June 7, 2005, p. A1.
MCI - laptop stolen from a car that was parked in the garage at the home of a MCI financial analyst	May 2005	current and former employees	16,500	names and SSNs	Young, Shawn, "MCI Reports Loss Of Employee Data On Stolen Laptop," <i>Wall Street Journal</i> , May 23, 2005, p. A2.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Florida International University (FIU) - a hacker acquired user names and passwords for 165 computers on campus	May 2005	faculty and students	unknown	SSNs, credit card numbers	Leyden, John, "Florida Univ on Brown Alert after Hack Attack," <i>The Register</i> , April 29, 2005, at [http://www.theregister.com/2005/04/29/fiu_id_fraud_alert/].
Time Warner - loss of 40 computer backup tapes containing sensitive data while being shipped by Iron Mountain to an offsite storage center	May 2005	current and former employees, some of their dependents and beneficiaries, and individuals who provided services for the company	600,000	names, SSNs	Zeller, Tom, "Time Warner Says Data on Employees Is Lost," <i>New York Times</i> , May 3, 2005, p. C4.
Carnegie Mellon University - security breach of school's computer network	May 2005	graduates of the Tepper School of Business from 1997 to 2004; current graduate students; applicants to the doctoral program from 2003 to 2005; applicants to the MBA program from 2002 to 2004; and administrative employees	5,000	SSNs and personal information	Associated Press, "Carnegie Mellon Reports Computer Breach," <i>MSNBC</i> , April 21, 2005, at [http://msnbc.msn.com/id/7590506/].

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
New Jersey cybercrime ring stole financial records from bank accounts	May 2005	customers of four banks (Charlotte, North Carolina-based Bank of America and Wachovia, Cherry Hill, New Jersey-based Commerce Bank, and PNC Bank of Pittsburgh)	700,000	names, SSNs, bank account information <b>note:</b> bank employees sold financial records to collection agencies and law firms.	Weiss, Todd, "Scope of Bank Data Theft Grows to 676,000 Customers: Bank Employees Used Computer Screen Captures to Snag Customer Data," <i>Computerworld</i> , May 20, 2005, at <a href="http://www.computerworld.com/security/topics/security/cybercrime/story/0,10801,101903,00.html">http://www.computerworld.com/security/topics/security/cybercrime/story/0,10801,101903,00.html</a> ].
Ameritrade (securities broker) - loses tapes with back-up information on customer accounts	April 2005	Ameritrade current and former customers	200,000	account information	"Ameritrade Loses Customer Account Info," <i>CNN Money</i> , April 19, 2005, at <a href="http://money.cnn.com/2005/04/19/technology/ameritrade/index.htm">http://money.cnn.com/2005/04/19/technology/ameritrade/index.htm</a> ].
Tufts University - possible security breach in an alumni and donor database after abnormal activity on the server in October and December, 2004	April 2005	alumni	106,000	SSNs and other unspecified personal information	Roberts, Paul "Tufts Warns 106,000 Alumni, Donors of Security Breach: Personal Data on a Server Used for Fund Raising May Have Been Exposed," <i>Computerworld</i> , April 13, 2005, at <a href="http://www.computerworld.com/security/topics/security/privacy/story/0,10801,101043,00.html?source=x101">http://www.computerworld.com/security/topics/security/privacy/story/0,10801,101043,00.html?source=x101</a> ].

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
HSBC (global bank) sent out warning letters notifying customers that criminals may have gained access to credit card info	April 2005	holders of General Motors MasterCard who had shopped at Polo Ralph Lauren	180,000	credit card information	"Security Score Hits HSBC's Cards," <i>BBC News</i> , April 14, 2005, at <a href="http://news.bbc.co.uk/2/hi/business/4444477.stm">http://news.bbc.co.uk/2/hi/business/4444477.stm</a> ; and Vijayan, Jaikumar, "Update: Scope of Credit Card Security Breach Expands," <i>Computerworld</i> , April 15, 2005, at <a href="http://www.computerworld.com/securitytopics/security/story/0,10801,101101,00.html">http://www.computerworld.com/securitytopics/security/story/0,10801,101101,00.html</a> .
San Jose Medical Group Management - desktop computers stolen from locked administrative office	April 2005	former patients from last 7 years	185,000	names, addresses, SSNs, confidential medical information	Weiss, Todd, "Update: Stolen Computers Contain Data on 185,000 Patients," <i>Computerworld</i> , April 8, 2005, at <a href="http://www.computerworld.com/databases/topics/data/story/0,10801,100961,00.html">http://www.computerworld.com/databases/topics/data/story/0,10801,100961,00.html</a> .
University of California, San Francisco - hacker gained access to server used by accounting and personnel department	April 2005	students, faculty and staff	7,000	names and SSNs numbers	Lazarus, David, "Another Incident for UC," <i>San Francisco Chronicle</i> , April 6, 2005, p. C1.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of California, Berkeley laptop stolen from restricted area of campus office	March 2005	alumni, graduate students, and past applicants	100,000	SSNs numbers, names, addresses, and birth dates for 1/3 of affected people	Liedtke, Michael, "Laptop Theft Causes Identity Fraud Worry," <i>Daily Breeze</i> (Torrance, CA), March 28, 2005, p. A10.
University Nevada, Las Vegas - hackers accessed school's Student and Exchange Visitor Information System (SEVIS) database	March 2005	current and former students and faculty	5,000	personal records, including birth dates, countries of origin, passport numbers, and SSNs	Lipka, Sara, "Hacker Breaks Into Database for Tracking International Students at UNLV," <i>Chronicle of Higher Education</i> , March 21, 2005, p. A43.
California State University, Chico - hackers broke into servers	March 2005	students, former students, prospective students, and faculty	59,000	SSNs	Associated Press, "Hackers Gain Personal Information of 59,000 People Affiliated with California University," <i>Grand Rapids Press</i> , March 22, 2005, p. A2.
LEXIS/NEXIS - intruders used passwords of legitimate customers to get access to a Seisint database called Accurint, which sells reports to law-enforcement agencies and businesses. Later analysis determined that its databases had been fraudulently breached 59 times using stolen passwords.	March 2005	customers	32,000 (subsequent investigation reveals the actual number is 310,000)	names, addresses, passwords, SSNs, drivers license	El-Rashidi, Yasmine, "LexisNexis Reports Data Breach; Personal Records Are Hacked as Concerns About Security and Identity Theft Intensify," <i>Wall Street Journal</i> , March 10, 2005, p. A3; and Krinn, Jonathan, "LexisNexis Data Breach Bigger Than Estimated: 310,000 Consumers May Be Affected, Firm Says," <i>Washington Post</i> , April 13, 2005, p. E1.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
DSW Shoe Warehouse store - information stolen from computer database over 3- month period	March 2005	customers of 103 of the chain's 175 stores	initially "hundreds of thousands," then raised to 1.4 million	credit card information	Associated Press, "DSW ID Theft May Affect Over 100,000," <i>Chicago Tribune</i> , March 11, 2005, p. 4; and "Firm Raises Data Theft Count," <i>Washington Post</i> , April 19, 2005, p. E2.
Bank of America - computer data tapes lost during shipment	February 2005	GSA charge card program (Visa cards issued to federal employees)	1.2 million	customer and account information	Carrns, Ann, "Bank of America Is Missing Tapes With Card Data," <i>Wall Street Journal</i> , February 28, 2005, p. B2.
ChoicePoint - criminals used fake documentation to open 50 fraudulent accounts to access consumer data	February 2005	consumers	30,000-35,000 in California; 145,000 nationwide	names, addresses, SSNs, credit reports	Perez, Evan, "ChoicePoint Is Pressed to Explain Database Breach," <i>Wall Street Journal</i> , February 5, 2005, p. A6.
T-Mobile - hacker intrusion into company database	February 2005	T-Mobile customers	400	customer records, passwords, SSNs, private e-mail and candid celebrity photos note: data offered for sale via online forum	Poulsen, Kevin, "Known Hole Aided T-Mobile Breach," <i>Wired News</i> , February 28, 2005, at [ <a href="http://www.wired.com/news/private/0,1848,66735,00.html">http://www.wired.com/news/private/0,1848,66735,00.html</a> ].

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of California, San Diego (UCSD) - hacker breached computer system	January 2005	students and alumni of UCSD Extension	3,500	names, SSNs	Yang, Eleanor, "Hacker Breaches Computers That Store UCSD Extension Student Alumni Data," <i>San Diego Union Tribune</i> , January 18, 2005, p. B3.
George Mason University - hackers gained access to information	January 2005	faculty, staff, and students	30,000	names, photos, SSNs, and campus ID numbers	McCullagh, Declan, "Hackers Steal ID Info from Virginia University," <i>Wired News</i> , January 10, 2005, at [ <a href="http://news.com.com/2100-7349_3-5519592.html">http://news.com.com/2100-7349_3-5519592.html</a> ].
Wells Fargo - computers stolen from Wells Fargo vendor	November 2004	mortgage and student-loan customers	company would not disclose	customers' names, addresses, and SSNs, and account numbers	Breyer, R. Michelle, "Wells Fargo Customer Data Stolen in Computer Theft," <i>Austin-American Statesman</i> , November 3, 2004, p. D1.
Affiliated Computer Services - inmate hacked into county database	October 2004	county employees	900	names, birth dates, SSNs, bank account routing numbers and checking account numbers	Whaley, Monte, "FBI on Weld ID-Theft Case Feds to Analyze Data from Cell of Inmate Who Hacked Computer," <i>Denver Post</i> , November 11, 2004, p. B1.
University of California, Berkeley - hacker compromised the university's computer system	October 2004	Californians participating in California's In-Home Supportive Services program since 2001	1.4 million individuals	SSNs, names, addresses, phone numbers, and dates of birth	Reuters, "Hacker Strikes University Computer System," <i>CNET News</i> , October 19, 2004, at [ <a href="http://news.com.com/2100-7349_3-5418388.html">http://news.com.com/2100-7349_3-5418388.html</a> ].

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
California State - auditor from chancellor's office lost hard drive containing personal information	August 2004	380,000 current and former students, applicants, staff, faculty and alumni at UC San Diego and 178,000 at San Diego State	23,500	name, address, SSNs	Connell, Sally Ann, "Security Lapses, Lost Equipment Expose Students to Possible ID Theft; in the Latest Incident, a Cal State Hard Drive with Data on 23,500 Individuals Is Missing." <i>Los Angeles Times</i> , August 29, 2004, p. B4.
Lowe's (home improvement store) - hacker used vulnerable wireless network to attempt to steal credit card info	June 2004	customers	unknown	skinned credit account information for every transaction processed at a particular Lowe's store	Roberts, Paul, "Wireless Hacker Pleads Guilty: Man Admits Using Store's Wireless Network to Steal Credit Card Info," <i>PC World</i> , June 7, 2004, at <a href="http://msn.pcworld.com/news/article/0,aid,116411,00.asp">http://msn.pcworld.com/news/article/0,aid,116411,00.asp</a> .
University of California, Los Angeles - stolen laptop w/ blood donor info	June 2004	blood donors	145,000	names, birth dates and SSNs	Becker, David, "UCLA Laptop Theft Exposes ID Info," <i>CNET News</i> , October 6, 2004, at <a href="http://news.com.com/UCLA+laptop+theft+exposes+ID+info/2100-1029_3-5230662.html?tag=nl">http://news.com.com/UCLA+laptop+theft+exposes+ID+info/2100-1029_3-5230662.html?tag=nl</a> .

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of California, San Diego (UCSD) - hackers breached security at the San Diego Supercomputer Center and the University's Business and Financial Services Department	April 2004	UCSD students, alumni, faculty, employees and applicants	380,000	SSNs, and driver license numbers	Sidener, Jonathan, "SD Supercomputer Center Among Victims of Intrusion," <i>San Diego Union Tribune</i> , April 15, 2004, p. B3.
eBay - hackers tricked online merchants who used the PayPal payment processing system into disclosing their user names and passwords, then logged onto the merchants' accounts	March 2004	several eBay merchants	company did not disclose	customer names, e-mail addresses, home addresses and transactions	Kirby, Carrie, "New Scam Threat at eBay / Hackers Obtained Information on Some Customers," <i>San Francisco Chronicle</i> , March 16, 2004, p. C1.
Illinois Employment Development Department server - hackers broke into	February 2004	people who work as domestic employees and those who employ them	90,000	SSNs; wages	"Hackers Breach State Files on 90,000," <i>Chicago Tribune</i> , February 15, 2004, p. 12.
Wells Fargo - hacker arrested with stolen computers and laptop	November 2003	customers with personal lines of credit used for consumer loans and overdraft protection	company would not disclose	names, addresses, account and SSNs	"Suspect Is Arrested in Theft of Bank Data," <i>Los Angeles Times</i> , November 27, 2003, p. C2.
Kinko's - hacker installed a key logger to record every character typed on 13 Kinko's computers	November 2003	Customers at Internet terminals at 13 Kinko's copy shops in Manhattan	450	SSNs, names, passwords, credit cards, bank account data <b>note:</b> data was sold	Napoli, Lisa, "A Hacker Masters Keystroke Theft: Personal Data Stolen From 450 Victims," <i>International Herald Tribune</i> , August 9, 2003, p. 1.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Acxiom (marketing company) - hacker downloaded data	August 2003	clients include 14 of the top 15 credit card companies; 5 of the top 6 retail banks; IBM, Microsoft, and federal government	10% of clientele (no total number given)	passwords, personal, financial, and company information	Lee, W.A. "Hacker Breaches Acxiom Data," <i>American Banker</i> , August 11, 2003, p. 5.
U.S. Department of Defense - hackers downloaded Navy credit cards	August 2003	Navy's purchase card program, used to order routine office supplies	13,000	credit card numbers	Reddy, Anita, "Hackers Steal 13,000 Credit Card Numbers; Navy Says No Fraud Has Been Noticed," <i>Washington Post</i> , November 23, 2003, p. E1.
Weichert Financial Services - credit profiles were unlawfully accessed from internal computer system	May 2003	clients	3,774	credit reports; driver's license info	Associated Press, "Pair Accused of Fraud in Credit Reports' Theft: Allegedly Used Data to Buy Goods over the Internet," <i>The Record</i> (Bergen County, NJ), May 2, 2003, p. A10.
DirectTV - hacker stole trade secrets for access card	April 2003	DirectTV subscribers	50,000 customers used counterfeit access cards to watch programming without paying	details about the design and architecture of DirectTV's "Period 4" cards <b>note:</b> data was sold	"U. of C. Student Pleads Guilty to Theft of Direc TV Card Data; Trade Secrets Ended up on Hacker Site, Enabling Free Access," <i>Chicago Sun-Times</i> , April 30, 2003, p. 16.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Texas, Austin - computer hackers broke into database on multiple occasions	March 2003	current and former student, faculty and staff members, as well as job applicants	55,200	names, addresses, SSNs, email addresses, office phone numbers <b>note:</b> perpetrator claimed he did not distribute the numbers and had not used them "to anyone's detriment"	Read, Brock, "Hackers Steal Data From U. of Texas Database," <i>Chronicle of Higher Education</i> , March 21, 2003, p. 35.
Georgia Institute of Technology	March 2003	patrons of art and theatre program	57,000	credit card numbers	Lemos, Robert, "Data Thieves Strike Georgia Tech," <i>Wired News</i> , March 31, 2003, at [http://news.com/Data+thieves+strike+Georgia+Tech/2100-1002_3-994821.html?tag=nl].
Visa, MasterCard, American Express and Discover account numbers - hacker stole 8 million	February 2003	credit card customers	PNC Bank cancelled 16,000 cards; Citizens Bank cancelled 8,000-10,000 cards	ATM/debit/check cards	"PNC Cancels 16,000 Cards After Hacking Theft Incident," <i>Pittsburgh Post-Gazette</i> , February 20, 2003, p. C1.
Bronx identify theft ring filed thousands of fraudulent income tax returns	February 2003	income tax filers	not specified	SSNs <b>note:</b> ID theft ring obtained \$7million in tax refunds	Weiser, Benjamin, "19 Charged in Identity Theft That Netted \$7 Million in Tax Refunds," <i>New York Times</i> , February 5, 2003, p. B3.

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Kansas - hacker break-in to Student and Exchange Visitor Information System (SEVIS)	January 2003	foreign students	1,400	SSNs, passport numbers, countries of origin, and birth dates.	Arnone, Michael, "Thacker Steals Personal Data on Foreign Students at U. of Kansas," <i>Chronicle of Higher Education</i> , January 24, 2003.
TriWest Healthcare Alliance - theft of a database containing names and SSNs	December 2002	military personnel and their dependents	500,000	names, addresses, SSNs	Gorman, Tom, "Reward Offered in Huge Theft of Identity Data; Stolen Computers Had Names, Social Security Numbers of 500,000 Military Families," <i>Los Angeles Times</i> , January 1, 2003, p. 14.
TCI help-desk worker sold client access codes to two others, who then used the codes to obtain more than 15,000 customer credit records	November 2002	credit reporting bureau customers	15,000 ( <i>Wired News</i> ) 30,000 ( <i>Seattle Times</i> )	names, addresses, SSNs, credit card <b>note:</b> data sold, for \$60 per record	Delio, Michelle, "Cops Bust Massive ID Theft Ring," <i>Wired News</i> , November 25, 2002, at [ <a href="http://www.wired.com/news/privacy/0,1848,56567,00.html">http://www.wired.com/news/privacy/0,1848,56567,00.html</a> ]; and Masters, Brooke, "Huge ID-Theft Ring Broken; 30,000 Consumers at Risk; Men Charged with Stealing Personal, Financial Data," <i>Seattle Times</i> , November 26, 2002, p. A1.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Midwest Express Airlines and Federal Aviation Administration - hackers posted list of customer names to website and posted a list of airport security screening results taken from the FAA's system	April 2002	Midwest Express Airlines customers; FAA (two separate incidents)	unknown	passenger names and airport security screening results	Larson, Virgil, "Computer Hackers Breach Midwest Express Systems," <i>Omaha World-Herald</i> , April 22, 2002, p. 1D.
ChoicePoint - Nigerian-born brother and sister posed as legitimate businesses to set up ChoicePoint accounts	2002	unknown	7,000-10,000 inquiries on names and SSNs; then used identities to commit fraud	names and SSNs <b>note:</b> data was sold	Associated Press, "ChoicePoint Suffered Previous Breach: Two ID Thieves Arrested in 2002 for Tapping into Data" <i>MSNBC</i> , February 3, 2005, at <a href="http://www.msnbc.msn.com/id/7065902/">http://www.msnbc.msn.com/id/7065902/</a> .
College of the Canyons (California) - computer hard drive containing personal student information stolen	October 2001	current and former students	36,000	names, SSNs, and photographs	Mistry, Bhavna, "Identity Theft Alert Issued at College," <i>Los Angeles Daily News</i> , October 21, 2001, p. NT.
Fullerton, California - bogus credit card ring which opened bank accounts, credit lines, auto and home loans	June 2001	impersonated more than 1,500 people nationwide and defrauded 76 financial institutions	1,500	birth dates, SSNs, mothers' maiden names, credit cards, driver's licenses, and receipts for car and home purchases.	Brown, Aldrin and Jeff Collins, "Suspicious Mail Triggered Probe of Identity Theft Crime Losses from the Alleged Ring, Which Used Data Stolen as Far Back as the Early '90s, May Hit \$10 Million," <i>Orange County Register</i> , June 21, 2001.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
New York City restaurant busboy duped credit reporting companies into providing detailed credit reports	March 2001	chief executives, celebrities and tycoons from Forbes list of richest Americans	200	SSNs, home addresses and birth dates, credit card numbers	Hays, Tom, "Busboy Hacks Only the Richest, Used Forbes' List in Plot to Steal Identity, Credit Info, Big Bucks." <i>Pittsburgh Post-Gazette</i> , March 21, 2001, p. A11.
World Economic Forum - hackers broke into computer	February 2001	attendees	3,200	passport numbers, cell phone numbers, credit card numbers, exact arrival and departure times, hotel names, room numbers, number of overnights, sessions attended, plus information on 27,000 people who have attended the global forum in recent years	Higgins, Alexander, "Hackers Steal World Leaders' Personal Data," <i>Chicago Sun-Times</i> , February 6, 2001, p. 20.
International credit card ring adds fraudulent charges of 277 Russian rubles (\$5-10) to credit cards	January 2001	Internet shopping sites	unknown	credit card numbers <b>note:</b> data was sold	James, Michael, "Small-time Thiefs Reap Big Net Gain Tens of Thousands of Phony \$5-\$10 Credit-Card Charges Rake in Millions for Hackers," <i>Orlando Sentinel</i> , January 27, 2001, p. E5.
University of Washington Medical Center - hacker broke into computer system	December 2000	cardiology and rehabilitation patients	5,000	names, addresses, birth dates, heights and weights, SSNs, and the medical procedure undergone	"Hacker Steals Patient Records," <i>San Diego Union-Tribune</i> , December 9, 2000, p. A3.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Egghead - hacker attacked computer system	December 2000	customers	3.5 million credit card accounts; 7500 of which showed "suspected fraudulent activity"	credit card info	"Sayer, Peter, "Egghead Says Customer Data Safe After Hack Attack," <i>PC World</i> , January 8, 2001 at <a href="http://nssn.pcworld.com/news/article/0,aId.37781,00.asp">http://nssn.pcworld.com/news/article/0,aId.37781,00.asp</a> ].
Western Union - hackers made electronic copies of the credit and debit card information	September 2000	customers who transferred money on a company website	15,700	credit and debit card information	Cobb, Alan, "Hackers Steal Credit Card Info from Western Union Site," <i>Chicago Sun-Times</i> , September 11, 2000, p. 22.
America Online - AOL customer-service representatives mistakenly downloaded an e-mail attachment sent by hackers	June 2000	customers	500 records were viewed	names, addresses, and credit card numbers	"Hackers Breach Security At America Online Inc," <i>Wall Street Journal</i> , June 19, 2000, p. A34.
Two British teens intruded into 9 e-commerce websites in the United States, Canada, Thailand, Japan and Britain	March 2000	customers	26,000 credit card accounts	credit card data <b>note:</b> some data was posted on the Web	Sniffen, Michael, "2 Teens Accused of Hacking Charged in \$3 Million Credit Card Theft," <i>Chicago Sun-Times</i> , March 25, 2000, p. 9.
CD Universe (online music store) - hacker stole credit card numbers and released thousands of them on a website when the company refused to pay a \$100,000 ransom	January 2000	customers	300,000	credit card numbers <b>note:</b> Maxus Credit Card Pipeline website posted up to 25,000 stolen numbers	Associated Pres, "Hacker Said to Steal 300,000 Card Numbers," <i>Arizona Republic</i> , January 11, 2000, p. A3.

CRS-29

Incident	Date Published	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Pacific Bell - 16-year-old teenager hacked into server and stole passwords	January 2000	subscribers	63,000 accounts were decrypted; 330,000 customers told to change passwords	passwords	Getteman, Jeffrey, "Passwords of PacBell Net Accounts Stolen; Computers: Authorities Say 16-year-old Hacker Took the Data for Fun: Theft Affects 63,000 Customers," <i>Los Angeles Times</i> , January 12, 2000, p. 2.

Source: This table was prepared by CRS from publicly available and news media sources.

Note: URLs are listed for exclusively online sources; other publications are identified by name and date.

