United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2007

PERSONAL INFORMATION

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

GAO-07-737

June 2007

PERSONAL INFORMATION

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-737, a report to congressional requesters

Why GAO Did This Study

In recent years, many entities in the private, public, and government sectors have reported the loss or theft of sensitive personal information. These breaches have raised concerns in part because they can result in identity theft—either account fraud (such as misuse of credit card numbers) or unauthorized creation of new accounts (such as opening a credit card in someone else's name). Many states have enacted laws requiring entities that experience breaches to notify affected individuals, and Congress is considering legislation that would establish a national breach notification requirement.

GAO was asked to examine (1) the incidence and circumstances of breaches of sensitive personal information; (2) the extent to which such breaches have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. To address these objectives, GAO reviewed available reports on data breaches, analyzed 24 large data breaches, and gathered information from federal and state government agencies, researchers, consumer advocates, and others.

What GAO Recommends

This report contains no recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-737.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David G. Wood at (202) 512-8678 or woodd@gao.gov.

What GAO Found

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches were reported in the news media from January 2005 through December 2006, according to lists maintained by private groups that track reports of breaches. These incidents varied significantly in size and occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities.

The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts. For example, in reviewing the 24 largest breaches reported in the media from January 2000 through June 2005, GAO found that 3 included evidence of resulting fraud on existing accounts and 1 included evidence of unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, there was not sufficient information to make a determination.

Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges. Notification requirements can create incentives for entities to improve data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach. Also, consumers alerted to a breach can take measures to prevent or mitigate identity theft, such as monitoring their credit card statements and credit reports. At the same time, breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals. Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether. Federal banking regulators and the President's Identity Theft Task Force have advocated a notification standard—the conditions requiring notification—that is risk based, allowing individuals to take appropriate measures where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

Contents

Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FTC	Federal Trade Commission
SSN	Social Security number
USPIS	United States Postal Inspection Service
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 4, 2007

The Honorable Spencer Bachus
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Michael N. Castle
House of Representatives

The Honorable Darlene Hooley
House of Representatives

The Honorable Steven C. LaTourette
House of Representatives

The Honorable Dennis Moore
House of Representatives

As a result of advances in computer technology and electronic storage, many different sectors and entities now maintain electronic records containing vast amounts of personal information on virtually all American consumers. In recent years, a number of entities—including financial service firms, retailers, universities, and government agencies—have collectively reported the loss or theft of large amounts of sensitive personal information. Some of these data breaches—such as those involving TJX Companies and the Department of Veterans Affairs (VA)—have received considerable publicity and have highlighted concerns about the protections afforded sensitive personal information.[1] Policymakers, consumer advocates, and others have raised concerns that data breaches can contribute to identity theft, in which an individual's sensitive personal

[1]In January 2007, The TJX Companies, Inc., publicly disclosed a data breach that compromised sensitive personal information, including credit and debit card data, associated with more than 45 million customer accounts. In May 2006, VA reported that computer equipment containing sensitive personal information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised. See GAO, *Privacy: Lessons Learned About Data Breach Notification*, GAO-07-657 (Washington, D.C.: Apr. 30, 2007).

information is used fraudulently. The Federal Trade Commission (FTC), which is responsible for taking complaints from victims and sharing them with law enforcement agencies, has noted that identity theft is a serious problem—millions of Americans are affected each year, and victims may face substantial costs and time to repair the damage to their good name and credit record.

Although there is no commonly agreed-upon definition, the term "data breach" generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers.[2] Data breaches can take many forms and do not necessarily lead to identity theft. The term "identity theft" is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name. Depending on the type of information compromised and how it is misused, identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings.

Beginning with California in 2002, at least 36 states have enacted breach notification laws—that is, laws that require certain entities that experience a data breach to notify individuals whose personal information was lost or stolen. There is no federal statute that requires most companies or other entities to notify affected individuals of data breaches, although federal banking regulatory agencies have issued guidance on breach notification

[2]In this report we use "personally identifiable information" to refer to any information that can be used to distinguish or trace an individual's identity—such as name, Social Security number, driver's license number, and mother's maiden name—because such information generally may be used to establish new accounts, but not to refer to other "means of identification," as defined in 18 U.S.C. § 1028(7), including account information such as credit or debit card numbers.

to the banks, thrifts, and credit unions they supervise.[3] In addition, the Office of Management and Budget has issued guidance—developed by the President's Identity Theft Task Force—on responding to data breaches at federal agencies.[4] Because a number of bills have been introduced in Congress that would establish a national breach notification requirement, you asked us to review the costs and benefits of such a requirement and the link between data breaches and identity theft.[5] As agreed with your offices, this report examines (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements.

This report focuses on breaches of sensitive personal data that can be used to commit identity theft, and not on breaches of other sensitive data, such as medical records or proprietary business information. To address the first two objectives, we obtained and analyzed information on data breaches that have been reported in the media and aggregated by three

[3]*See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005). The five federal banking regulatory agencies are the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. The National Credit Union Administration issued its guidance (which was substantially identical) separately from the other four regulators (*see* Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, 70 Fed. Reg. 22764 (May 2, 2005)).

[4]The President's Identity Theft Task Force—chaired by the Attorney General and cochaired by the Chairman of the Federal Trade Commission and comprising 17 federal agencies and departments—was charged with developing a comprehensive national strategy to combat identity theft. Exec. Order No. 13,402, *Strengthening Federal Efforts to Protect Against Identity Theft*, 71 Fed. Reg. 27945 (May 10, 2006). The task force's guidance was distributed in a memorandum from the Office of Management and Budget to the heads of federal agencies and departments. *See* Office of Management and Budget Memorandum for the Heads of Departments and Agencies, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006. In May 2007, the Office of Management and Budget issued a memorandum that updated the September 2006 guidance and, among other things, required agencies to develop and implement breach notification policies within 120 days. *See* Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007).

[5]*See*, for example, Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); and Identity Theft Prevention Act, S. 1178, 110th Cong. (2007).

private research and advocacy organizations, as well as information on breaches collected by state agencies in New York and North Carolina, federal banking regulators, and federal law enforcement agencies.[6] We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee in 2006 and by the Department of Homeland Security (DHS).[7] In addition, we conducted a literature search of relevant articles, reports, and studies. We also conducted interviews with, and obtained documents from, representatives of federal agencies, including the FTC, the Department of Justice, DHS, and the federal banking regulatory agencies; selected state government agencies and the National Association of Attorneys General; private and nonprofit research organizations; and consumer protection and privacy advocacy groups. Further, we obtained information from industry and trade associations representing key sectors—including financial services, retail sales, higher education, health care, and information services—that have experienced data breaches. In addition, for the second objective, we examined the 24 largest (in terms of number of records breached) data breaches reported by the news media from January 2000 through June 2005 and tracked by private groups. For each of these breaches, we reviewed media reports and other publicly available information, and conducted interviews, where possible, with representatives of the entities that experienced the breaches, in an attempt to identify any known instances of identity theft that resulted from the breaches. We also examined five breaches that involved federal agencies, which were selected because they represented a variety of different circumstances. For the third objective, we reviewed the federal banking regulatory agencies' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law, which included interviewing and gathering information from California

[6]The three private organizations are Attrition, Identity Theft Resource Center, and Privacy Rights Clearinghouse. We reviewed data on breaches in New York and North Carolina because they represent two large states that maintain centralized information on data breaches.

[7]The House Government Reform Committee was renamed the House Oversight and Government Reform Committee in the 110th Congress.

state officials and selected California companies, educational institutions, and other entities subject to the law's notification requirements.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards. A more extensive discussion of our scope and methodology appears in appendix I.

Results in Brief

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches have been reported in the news media from January 2005 through December 2006, according to our analysis of lists maintained by three private organizations that track such breaches. Further, a House Government Reform Committee survey of federal agencies identified more than 788 data breaches at 17 agencies from January 2003 through July 2006. Of the roughly 17,000 federally supervised banks, thrifts, and credit unions, several hundred have reported data breaches to their federal regulators over the past 2 years. In addition, officials in New York State—which requires public and private entities to report data breaches to a centralized source—reported receiving notice of 225 breaches from December 7, 2005, through October 5, 2006. Data breaches have occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Some studies indicate that most publicly reported breaches resulted from intentional actions, such as a stolen laptop computer, rather than accidental occurrences, such as a lost laptop computer, but this may be because breaches related to criminal activity are perhaps more likely to be reported. Media-reported breaches have varied significantly in size, ranging from 10 records to tens of millions of records. Most of these breaches have compromised data that included personally identifiable information, while others have involved only account information such as credit card numbers.

The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the data used to commit identity theft. Although we identified several cases where breaches reportedly have resulted in identity theft—that is, account fraud or unauthorized creation of new accounts—available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, our review of the 24 largest

breaches that appeared in the news media from January 2000 through June 2005 found that 3 breaches appeared to have resulted in fraud on existing accounts, and 1 breach appeared to have resulted in the unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, we did not have sufficient information to make a determination. Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and it may be up to a year or more before stolen data are used to commit a crime. Some studies by private researchers have found little linkage between data breaches and identity theft, although our review found these studies had methodological limitations. Finally, the circumstances of a breach can greatly affect the potential harm that can result. For example, unauthorized creation of new accounts generally can occur only when a breach includes personally identifiable information. Further, breaches that are the result of intentional acts generally are considered to pose more risk than accidental breaches, according to federal officials.

Requiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft, but it also involves monetary costs and challenges such as determining an appropriate notification standard. Representatives of federal banking regulators, other government agencies, industry associations, and other affected parties told us that breach notification requirements have encouraged companies and other entities to improve their data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach of customer data. Further, notifying affected consumers of a breach gives them the opportunity to mitigate potential risk—for example, by reviewing their credit card statements and credit reports, or placing a fraud alert on their credit files. Some privacy advocates and others have noted that even when the risk of actual financial harm is low, breach notification is still important because individuals have a basic right to know how their personal information is being handled and when it has been compromised. At the same time, affected entities incur monetary costs to comply with notification requirements. For example, 31 companies that responded to a 2006 survey said they incurred an average of $1.4 million per breach, for costs such as mailing notification letters, call center expenses, courtesy discounts or services, and legal fees. In addition, organizations subject to notification requirements told us they face several challenges, including the lack of clarity in some state statutes about when a notification is required, difficulty identifying and locating affected individuals, and difficulty

complying with varying state requirements. Notification standards—that is, the circumstances surrounding a data breach that "trigger" the required notification—vary among the states. Some parties, such as the National Association of Attorneys General, have advocated that a breach notification requirement should apply broadly in order to give consumers a greater level of protection and because the risk of harm is not always known. The guidance provided by federal banking regulators lays out a more risk-based approach, aimed at ensuring that affected individuals receive notices only when they are at risk of identity theft or other related harm. Such an approach was also adopted by the President's Identity Theft Task Force, which recommended a risk-based standard for breach notification applicable to both government agencies and private entities. As we have noted in the past, care is needed in defining appropriate criteria for incidents that merit notification. Should Congress choose to enact a federal breach notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

This report contains no recommendations. We provided a draft of this report to FTC and provided selected portions of the draft to federal banking regulatory agencies and relevant federal law enforcement agencies. These agencies provided technical comments, which we have incorporated in this report as appropriate.

Background

Breaches of sensitive personal data in recent years at companies, universities, government agencies, and other organizations have heightened public awareness about data security and the risks of identity theft, and have led to the introduction of breach notification requirements in many state legislatures. As of April 2007, at least 36 states had enacted some form of law requiring that affected individuals be notified in the event of a data breach; California's law, enacted in 2002, was the first such state requirement.[8] States' notification requirements vary, particularly with regard to the applicable notification standard—the event or circumstance that triggers a required notification. Requirements also vary in terms of the data to which they apply—for example, some apply to paper documents as well as electronic records.

[8]Cal. Civ. Code § 1798.82.

There is currently no federal statute that requires most companies and other entities that experience a data breach to notify individuals whose personal information was lost or stolen. However, the Gramm-Leach-Bliley Act established requirements for federally supervised financial institutions to safeguard customer information.[9] To clarify these requirements, the federal banking regulators issued interagency guidance in 2005 to the banks, thrifts, and credit unions they supervise related to their handling of data breaches. Under this guidance, these institutions are expected to develop and implement a response program to address unauthorized access to customer information maintained by the institution or its service providers; and if they experience a breach, they are to notify their primary federal regulator as soon as possible and—depending on the circumstances of the incident—notify their affected customers. In addition, in September 2006 the President's Identity Theft Task Force developed guidance for federal agencies on responding to breaches involving agency data, including the factors to consider in determining whether to notify affected individuals. The task force released a strategic plan for combating identity theft in April 2007, which contained among its recommendations a proposal for establishing a national breach notification requirement.[10] Further, in December 2006, the Department of Veterans Affairs Information Security Enhancement Act of 2006 became law, which, among other things, requires VA to prescribe regulations providing for the notification of data breaches occurring at the department.[11] A number of bills have been introduced in Congress that would more broadly require companies and other entities to notify

[9]Pub. L. No. 106-102, tit. V, subtit. A, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. § 6801-6809).

[10]President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: Apr. 11, 2007).

[11]Pub. L. No. 109-461, tit. IX, 120 Stat. 3450 (Dec. 22, 2006), *codified at* 38 U.S.C. § 5721-5728, 7901-7907.

individuals when such breaches occur, and Congress has held several hearings related to data breaches.[12]

Identity theft occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.[13] There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use identifying data, which can include such things as SSNs and driver's license numbers, to open new financial accounts and incur charges and credit in an individual's name, without that person's knowledge. This second form of identity theft is potentially the most damaging because, among other things, it can take some time before a victim becomes aware of the problem, and it can cause substantial harm to the victim's credit rating. While some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. According to FTC, millions of Americans have their identities stolen each year. Roughly 85 percent of these cases involve the misuse of existing accounts and 35 percent involve new account creation or other fraud. (Twenty percent of the total involve both.) Identity thieves obtain sensitive personal information using a variety of methods. One potential source is a breach at an organization that maintains large amounts of sensitive personal information. However, identity theft can also occur as a result of the loss or theft of data maintained by an individual, such as a lost or stolen wallet or a thief digging through household trash.

[12]For example, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 109th Cong., 1st Sess. (2005); *Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary*, 109th Cong., 1st Sess. (2005); *Assessing Data Security: Preventing Breaches and Protecting Sensitive Information: Hearing Before the House Comm. on Financial Services*, 109th Cong., 1st Sess. (2005); *Securing Consumers' Data: Options Following Security Breaches: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 109th Cong., 1st Sess. (2005).

[13]For additional information on identity theft, see GAO, *Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Under Way*, GAO-05-710 (Washington, D.C.: Jun. 30, 2005) and *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime and charged FTC with taking complaints from identity theft victims; sharing these complaints with federal, state, and local law enforcement agencies; and providing the victims with informational materials to assist them.[14] Because identity theft is typically not a stand-alone crime but rather a component of one or more crimes such as bank fraud, credit card fraud, and mail fraud, a number of federal law enforcement agencies can have a role in investigating identity theft crimes, including the Federal Bureau of Investigation (FBI), U.S. Postal Inspection Service (USPIS), U.S. Secret Service (Secret Service), the Office of the Inspector General of the Social Security Administration, and Immigration and Customs Enforcement.

Available Evidence Indicates That Data Breaches Occur Frequently and Under Varying Circumstances

Available evidence from media reports, federal and state agencies, and private institutions, collectively, suggests that data breaches occur with some frequency. For example, our analysis of the lists of data breaches compiled by three private research and advocacy organizations shows more than 570 breaches reported by the news media from January 2005 through December 2006. Data breaches have occurred across a range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Breaches have varied in size and have resulted from both criminal actions and accidental incidents. Most of the breaches reported in the news media have involved data that included personal identifiers such as SSNs, while others have involved only account information such as credit card numbers.

Several Sources Indicate That Breaches of Sensitive Personal Information Are Frequent

No federal agency or other organization tracks all data breaches, and definitions of what constitutes a data breach may vary. Although there are no comprehensive data on the extent of data breaches nationwide, government officials, trade association representatives, researchers, and consumer and privacy advocates we interviewed agreed that breaches of sensitive personal information occur frequently. For example, representatives of a variety of organizations—including the Department of

[14]Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998). In addition to FTC, other federal agencies maintain data on identity theft. For example, the Internet Crime Complaint Center, a joint venture of the FBI and the National White Collar Crime Center, receives Internet-related identity theft complaints, which it shares with law enforcement agencies throughout the country.

Justice, California's Office of Privacy Protection, the Consumer Data Industry Association (a trade group representing many information resellers), and the Ponemon Institute (a private research organization)—characterized data breaches in the United States as being "prevalent" or "common." Although we did not identify comprehensive data on the extent of data breaches, available information from several sources does corroborate the anecdotal evidence that such breaches occur frequently.[15]

Media Reports

Over the past few years, several hundred data breaches have been reported each year by newspapers and other news media. Three private organizations that focus on information privacy and security issues—Privacy Rights Clearinghouse, Identity Theft Resource Center, and Attrition—track data breaches reported in newspapers, magazines, and other publicly available sources of news and information.[16] Our analysis of the three lists of data breaches maintained by these organizations indicated that at least 572 breaches were reported in the news media from January 2005 through December 2006.[17] These breaches were reported to

[15]Because the breaches cited in this section of the report derive from different sources, there may be some overlap among the numbers cited by these sources.

[16]Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings. Identity Theft Resource Center is a nonprofit organization that provides consumer and victim support and advises governmental agencies, legislators, and companies on the issue of identity theft. Attrition is an information security-related Web site maintained by volunteers.

[17]Representatives of these three organizations indicated that their definition of a data breach was consistent with the definition used in this report. However, we did not independently confirm whether the individual breaches reported by the media and tracked by these groups met the criteria for this definition, and it is possible that some of them do not. We reviewed these lists as they appeared as of February 15, 2007; additional breaches that occurred during the 2-year period we reviewed may have been subsequently added as they were discovered. Our analysis eliminated overlap among the three lists; the 572 breaches we cite represent unique breaches that appeared on at least one list.

have affected more than 80 million records.[18] However, for several reasons, these lists likely understate the true extent of data breaches in the United States. First, organizations might not voluntarily disclose data breaches that they experience. Second, some breaches that organizations do disclose may not appear in the news media, particularly if the breach was limited in scope. Finally, the three organizations compiling these lists may not have identified all of the breaches reported in the news media—for example, many breaches did not appear on all three lists, suggesting that none represents an exhaustive list of all breaches that have appeared in the news.

Federal Law Enforcement Agencies

Officials at federal law enforcement agencies told us that each year they conduct a significant number of criminal investigations that involve alleged breaches of sensitive personal information. For example, officials of the FBI's Cyber Division told us that presently it has more than 1,300 pending cases of computer or network intrusions where data breaches resulted from unauthorized electronic access to computer systems, such as hackings, at public and private organizations.[19] Officials at the Secret Service, which investigates certain cases where financial information has been lost or stolen, told us that in 2006, the service opened 327 cases involving network intrusions or other breaches at retailers, banks, credit card processors, telephone companies, educational institutions, and other organizations. Officials noted that they have seen a steady increase in the number of data breaches since 1986, when they began tracking computer fraud violations. Investigators at USPIS, the division of the U.S. Postal

[18]There were 83 million records collectively reported to have been affected by the 572 breaches. However, in some cases, the number of records affected was unknown or unreported, and the total does not reflect those breaches. Also, the number of breached records containing personal information may not be the same as the number of individuals affected by breaches because some individuals may be victims of more than one breach or may have multiple records compromised in a single breach. Finally, in addition to the 83 million records, as many as 40 million additional records may have been affected by a single breach involving the credit card processor CardSystems, although the exact number of affected records is unclear. In a complaint following the breach, FTC alleged that a hacker obtained unauthorized access to magnetic stripe data for tens of millions of credit and debit cards. However, according to testimony by a CardSystems official, only 263,000 of these records (containing 239,000 discrete account numbers) included sensitive personal information.

[19]According to these officials, not all 1,300 pending computer intrusion cases necessarily involved breaches that compromised sensitive personal information, although the vast majority have. The term hacking is commonly used to refer to accessing a computer system without authorization, with the intention of destroying, disrupting, or carrying out illegal activities on the network or computer system.

Service that investigates mail fraud, external mail theft, fraudulent changes of addresses, and other postal-related crimes, told us that the agency does not specifically track the number of data breaches in the private sector. However, despite limited data, investigators said their impression is that such data breaches likely occur frequently.

House Government Reform Committee and DHS

To obtain information on the prevalence of data breaches at federal agencies, in July 2006 the House Government Reform Committee asked federal agencies to provide details about incidents involving the loss or compromise of any sensitive personal information held by an agency or contractor from January 1, 2003, through July 10, 2006. Our analysis of the committee's report found that 17 agencies reported that they experienced at least one breach and, collectively, the agencies reported to the committee more than 788 separate incidents.[20]

The Federal Information Security Management Act of 2002 requires all federal agencies to report computer security incidents to a federal incident response center.[21] The U.S. Computer Emergency Readiness Team—a component of DHS that monitors computer security incidents at federal agencies—serves as this response center. As such, data breaches at federal agencies involving certain sensitive information must be reported to the

[20]Government Reform Committee, U.S. House of Representatives, *Staff Report: Agency Data Breaches Since January 1, 2003* (Washington, D.C.: Oct. 13, 2006). The federal agencies covered in the report were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, as well as the Office of Personnel Management and the Social Security Administration. In addition to 788 incidents reported by 16 federal agencies, the Committee received information on data breaches from the Department of Veterans Affairs, which the report characterized only as "hundreds" of incidents.

[21]Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (Dec. 17, 2002), *codified at* 44 U.S.C. § 3541-3549; 40 U.S.C. § 11331.

team within 1 hour of discovery of the incident.[22] DHS staff told us that they receive information about breaches at federal agencies on a daily basis. In fiscal year 2006, the center tracked 477 incidents at 59 federal agencies or at federal contractors with access to government-owned data, according to information available as of January 29, 2007. In addition, a March 2007 audit investigation found that at least 490 laptop computers owned by the Internal Revenue Service and containing taxpayer information had been lost or stolen since 2003.[23]

Federal Banking Regulators

The 2005 guidance issued by the five federal banking regulators provided that a depository institution should notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to or use of sensitive customer information.[24] The guidance applies to breaches that have occurred at the financial institutions themselves, as well as third-party entities such as data processors that act as service providers and maintain customer information.[25] The five regulators differ in their methods and criteria for tracking breaches, but collectively they have tracked several hundred breaches over the past few years at roughly

[22]Office of Management and Budget Memorandum for Chief Information Officers, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, M-06-19 (July 12, 2006). The U.S. Computer Emergency Readiness Team defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practice" and the Office of Management and Budget requires reporting if the incident includes personally identifiable information, which under its definition refers to "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

[23]Treasury Inspector General for Tax Administration, *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices*, Ref. No. 2007-20-048 (Washington, D.C.: Mar. 23, 2007).

[24]70 Fed. Reg. 15736 (Mar. 29, 2005) and 70 Fed. Reg. 22764 (May 2, 2005).

[25]Only data breaches at the financial institutions and at third-party entities that are their service providers and maintain their customer information are subject to the guidance; this requirement is codified at 12 C.F.R. Pt. 30, App. B, Supp. A § II(A)(2); 12 C.F.R. Pt. 208, App. D-2, Supp. A § II(A)(2); 12 C.F.R. Pt. 225, App. F, Supp. A § II(A)(2); 12 C.F.R. Pt. 364, App. B, Supp. A § II(A)(2); 12 C.F.R. Pt. 570, App. B, Supp. A § II(A)(2); and 12 C.F.R. Pt. 748, App. B § II(A)(2*)*. However, data collected by the regulators may also include some breaches that affected their institutions but were not covered by the guidance.

17,000 institutions they supervise and at third-party entities.[26] For example, the Federal Deposit Insurance Corporation (FDIC)—the primary federal supervisor for more than 5,000 state-chartered banks that are not members of the Federal Reserve System—received reports of 194 breaches at its regulated institutions from May 2005 through December 2006, as well as reports of 14 breaches at third-party companies that also affected these institutions' customers. Similarly, officials at the Office of Thrift Supervision—which supervises more than 860 savings associations—told us that from April 2005 through December 2006, 56 of its institutions reported breaches at the institution itself and approximately 72 reported breaches at third-party entities that maintained their customer information.

State Agencies

Some states require entities experiencing data breaches to report them to designated state agencies.[27] For example, the New York State Information Security Breach and Notification Act requires entities that experience security breaches to notify the state Attorney General's Office, Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination in cases when New York residents must be notified.[28] Such data breaches include the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of unencrypted private information. Officials of the Office of New York State Attorney General told us that from December 7, 2005, through October 5, 2006, their office received notice of 225 breaches. Similarly, a North Carolina law requires that breaches of personal information (maintained in computerized, paper, or other media) affecting at least 1,000 persons be reported to the Consumer Protection Division of the state Office of the Attorney General.[29] An official in that office told us that from December 2005 through December 2006, it had received reports of 91 breach incidents.

[26]Regulators note that while they track breaches occurring at third-party service providers involving customer information of regulated financial institutions, these breaches are typically due to lapses in data security by the third-party entity and not the financial institution itself.

[27]We did not determine the precise number of states with centralized reporting requirements. For illustrative purposes, we obtained information on data breaches from New York and North Carolina because they are two large states known to require that data breaches be reported to state agencies.

[28]N.Y. Gen. Bus. Law § 899-aa.

[29]N.C. Gen. Stat § 75-65.

Other Sources

Information that we obtained from several other sources suggests that breaches of sensitive personal information occur with some frequency across a variety of sectors. For example,

- EDUCAUSE, a nonprofit association that addresses technology issues in higher education, conducted a survey in 2005 on data security at higher education institutions in the United States and Canada. Twenty-six percent of the 490 institutions that responded said they had experienced a security incident in the past year that resulted in the compromise of confidential information.[30]

- The American Hospital Association collected information, at our request, in October 2006 from a nonrepresentative group of 46 large hospitals on breaches of sensitive personal information (excluding medical records) that they had experienced since January 2003. Collectively, 13 of the 46 hospitals reported a total of 17 data breach incidents.[31]

- The Ponemon Institute, a private company that researches privacy and security practices, conducted a survey of 51,433 U.S. adults and received responses from 9,154 (a response rate of about 18 percent). About 12 percent of the survey respondents said they recalled receiving notification of a data security breach involving their personal information.[32]

- The CMO Council, an organization serving marketing executives, reported that 16 percent of consumers who responded to a Web-based panel reported that a company had lost or compromised their personal,

[30]EDUCAUSE Center for Applied Research, *Safeguarding the Tower: IT Security in Higher Education 2006*, Volume 6, 2006.

[31]The association received information from 46 of the 78 hospitals it surveyed, a response rate of 59 percent. As agreed in advance, to preserve confidentiality the association provided us with a summary of their findings but did not identify the hospitals, and we did not independently verify the data.

[32]Ponemon Institute, LLC, *National Survey on Data Security Breach Notification* (Sept. 26, 2005). The reliability of this study's findings may be limited by a low survey response rate.

financial, or medical information. An additional 32 percent of respondents said they were not sure.[33]

- Several other studies, while not focusing specifically on breaches of sensitive personal information, have found more generally that information security vulnerabilities are widespread among U.S. and global companies.[34]

Information from multiple sources indicates that data breaches at companies, government agencies, retailers, and other entities have occurred frequently in recent years, involving millions of records of sensitive personal information. We have reported in the past that no federal law explicitly requires most companies and other entities to safeguard all of the sensitive personal information they may hold. We also have suggested that to ensure that sensitive personal information is protected on a more consistent basis, Congress should consider expanding requirements to safeguard such information.[35] The frequency of data breaches identified in this report underscores the need for entities in the public and private sectors to improve the security of sensitive personal information and further corroborates that additional federal action may be needed in this area.

Source, Cause, Size, and Content of Breaches Have Varied Widely

According to government officials, researchers, and media reports, data breaches have occurred among a wide variety of entities and as a result of both intentional actions and accidental losses. These breaches also have varied in size and in the types of data compromised.

Type of Entity

Data breaches have been reported at a wide range of public and private institutions, including federal, state, and local government agencies; public

[33]CMO Council, *Securing the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation*, September 2006. The reliability of this study's findings may be limited because they are based on a self-selected group of respondents to a Web-based panel. Also, we were unable to determine a response rate because, according to a CMO Council representative, the total number of survey respondents was not available.

[34]For example, see Deloitte, *2006 Global Security Survey* (2006); Small Business Technology Institute, *Small Business Information Security Readiness* (San Jose, California: July 2005); Ponemon Institute, LLC, *U.S. Survey: Confidential Data at Risk* (Aug. 15, 2006); and Ponemon Institute, LLC, *Benchmark Study of European and U.S. Corporate Privacy Practices* (Apr. 26, 2006).

[35]GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: Jun. 26, 2006).

and private colleges and universities; hospitals and other medical facilities; retailers; banks and other financial institutions; information resellers; and others. For example, in the weeks leading up to the highly publicized 2005 CardSystems breach, the media also had reported breaches at, among other entities, a large hospital, a university, a global financial institution, a federal regulatory agency, and a major technology company.

According to Attrition, of the breaches it tracked as reported in the news media in 2005 and 2006, 33 percent of the breaches occurred at educational institutions, 32 percent at financial services institutions, 25 percent at government agencies, and 10 percent at medical facilities, although breaches reported in the news media may not be representative of all breaches.[36] Similarly, the data security firm ID Analytics examined 70 data breaches that were reported by the news media from February through September 2005. According to company officials, 46 percent of these breaches occurred at educational institutions, 16 percent at financial institutions, 14 percent at retailers, 11 percent at government agencies, 7 percent at medical facilities, and 6 percent at information resellers.[37]

Another way to analyze where data breaches have occurred is to look at the number of *records* breached (as opposed to the number of breaches themselves). Our analysis of the list maintained by Attrition found that 54 percent of breached records involved financial institutions, 34 percent involved government agencies, 4 percent involved educational institutions, and 3 percent involved medical facilities. ID Analytics' report found that 57 percent of breached records involved financial institutions, 22 percent involved retailers, 13 percent involved educational institutions, 4 percent involved information resellers, 2 percent involved government agencies, and 2 percent involved medical facilities.

Cause of Breach

According to government officials, researchers, and media reports, data breaches of sensitive personal information have occurred as a result of both intentional actions as well as negligence or accidental losses. In some cases, individuals intentionally steal information for the purpose of

[36]For our analysis, we used the categories provided by Attrition for the industry sector where the breach occurred. We did not independently verify the accuracy of these categorizations.

[37]ID Analytics, Inc., *National Data Breach Analysis* (San Diego, California: January 2006). The data we cite reflect a combination of data presented in the report and additional data provided to us by ID Analytics.

committing fraud or identity theft. Breaches involving intentional actions have included:

- *Hacking*, or accessing computer systems without authorization. For example, in 2007 the retailer TJX Companies reported unauthorized intrusions into its computer systems that may have breached millions of customers' credit card and driver's license information.

- *Employee theft*. For example, in 2006, a former employee of the American Red Cross pled guilty to stealing personally identifiable information from a blood donor database.

- *Theft of physical equipment*. In 2005, for instance, a laptop containing the names and SSNs of more than 98,000 students, alumni, and others was stolen from the University of California at Berkeley.

- *Deception or misrepresentation to obtain unauthorized data*. In 2005, the information reseller ChoicePoint acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services.

Breaches involving negligence or accidental losses of data have included the following:

- *Loss of laptop computers or other hardware*. For example, in 2006, the Department of Labor reported that an employee lost a laptop containing personal information on 1,137 individuals.

- *Loss of data tapes*. For example, in 2004, Bank of America lost backup tapes containing personal information of 1.2 million government charge card holders while the tapes were being transported to a data center.

- *Unintentional exposure on the Internet*. In 2006, according to media reports, the U.S. Department of Education left unprotected on a Web site the personally identifiable information, including SSNs, of up to 21,000 recipients of federal student loans.

- *Improper disposal of data*, such as leaving sensitive personal data on unshredded documents in a publicly accessible dumpster.

We did not identify comprehensive data that reliably provide overall statistics on the causes of known data breaches. However, our review of the 24 largest data breaches reported in the news media (discussed in

more detail later in this report) found that 12 breaches apparently involved intentional acts by hackers or employees illegally accessing or using data, 5 involved stolen laptops or other computer equipment, 4 involved lost computer backup tapes, 2 involved the use of deception to gain access to data, and 1 involved the possible unauthorized disclosure of data. In addition, some studies indicate that most breaches reported in the news media resulted from intentional acts rather than accidental occurrences such as a lost laptop computer. For example, in its study of 70 breaches, ID Analytics determined that 48 involved thefts committed with the apparent intention of accessing sensitive data. Eleven of the breaches involved thefts where sensitive consumer information was apparently stolen inadvertently as part of another crime (such as the theft of a laptop computer for its resale value), and another 11 breaches involved accidental loss (such as misplacement of a laptop computer). However, these data may overrepresent the proportion of all breaches that involve criminal activity, as such breaches are probably more likely than accidental losses to be reported to authorities and by the news media.

Number of Records Breached

Our analysis of the list maintained by Attrition of breaches reported by the news media found the median number of records breached to be 8,650. However, these data breaches varied considerably in size—ranging, for example, from a breach involving 10 records at a law firm to a breach involving as many as tens of millions of records at a credit card processing company. The breaches involving federal agencies that were reported to the House Government Reform Committee also varied in size—for example, several affected fewer than five records, while a breach at VA affected 26.5 million records.

Types of Data Breached

Comprehensive information does not exist on the types of data involved in all known data breaches. Among the list maintained by Attrition of breaches reported by the news media in 2005 and 2006—which may not be representative of all breaches—more than half involved SSNs and 11 percent involved credit card numbers (and 3 percent of the total involved both). In the remaining breaches, other types of account or personal information were involved, or the type of data breached was not reported. Logically, there may be an association between the type of data compromised and the type of entity experiencing the breach. For example, several educational institutions have experienced breaches of SSNs, which they may maintain as student identifiers, and several retail stores have experienced breaches of credit card numbers, which they often maintain on their customers.

Consequences of Data Breaches Are Not Fully Known, but Clear Evidence of Identity Theft Has Been Found in Relatively Few Breaches

Comprehensive information on the outcomes of data breaches is not available. Several cases have been identified in which a data breach appears to have resulted in identity theft, but available data and information from law enforcement and industry association representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, of 24 very large breaches we reviewed, 3 appeared to have resulted in fraud on existing accounts and 1 in the unauthorized creation of new accounts. Determining the link between data breaches and identity theft is challenging because, among other things, identity theft victims often do not know how their personal information was obtained. However, the circumstances of a breach, including the type of information compromised and how the breach occurred, can greatly affect the potential risk of identity theft.

Federal Law Enforcement Agencies and Industry Associations Identified Limited Instances of Breaches Leading to Identity Theft

In general, representatives of law enforcement agencies, industry and trade associations, and consumer and privacy advocacy organizations told us that no comprehensive data are available on the consequences of data breaches. Several cases have been identified where there is evidence that a data breach resulted in identity theft, including account fraud or unauthorized creation of new accounts. At the same time, available data and information from the officials we contacted indicated that most breaches have not resulted in detected incidents of identity theft.

We asked representatives of the FBI, Secret Service, USPIS, and Immigration and Customs Enforcement—a component of DHS that has investigated cases where stolen identities were used to secure jobs—the extent to which data breaches they investigated resulted in some form of identity theft. Representatives of all of these agencies told us that their investigations of data breaches do not typically allow them to fully ascertain how stolen data are used. Similarly, they noted that investigations of identity theft do not always reveal the source of the data used to commit the crime.

However, the representatives were able to provide us with a limited number of examples in which data breaches they investigated had allegedly resulted in some form of identity theft. For example, in a 2006 investigation by USPIS, an employee of a credit card call center allegedly compromised at least 35 customers' accounts and used some of the information to purchase approximately $65,000 in gift cards. The representatives of federal law enforcement agencies noted that cases in which data breaches have been linked to identity theft often have involved instances of unauthorized access by employees. For example, an official at

Immigration and Customs Enforcement stated that her agency, in cooperation with other agencies, has investigated cases in which government employees allegedly had improperly accessed and sold sensitive personal information that was then used by illegal immigrants to secure employment.

In addition, in 2005 FTC settled charges with BJ's Wholesale Club in which alleged security breaches resulted in several million dollars in fraudulent purchases using customers' credit and debit card data.[38] As discussed later in this report, FTC has also taken enforcement actions related to data breaches at several other companies, including ChoicePoint, CardSystems, and DSW, in which it uncovered evidence that the breaches resulted in identity theft.

Many of the law enforcement officials said that, based on their experience, data breaches that result in harm have usually involved fraud on existing accounts (such as credit card fraud) rather than the unauthorized creation of new accounts. Secret Service representatives noted that using illicit credit and debit card numbers and bank account information is much easier and less labor intensive than using personally identifiable information to fraudulently open new accounts. Officials at Secret Service, FBI, and USPIS all said that identity theft involving the creation of new accounts often results not from data breaches, but from other sources, such as retrieving personal information by sifting through a family's household trash.

In examining a selection of five breaches that occurred from 2003 through 2005 that were reported as having involved five federal agencies—Department of Justice, FDIC, Internal Revenue Service, National Park Service, and the Navy—we found that the circumstances behind these breaches varied widely. At least two of the breaches occurred at vendors or contractors that held sensitive data on agency employees, rather than at the agency itself. In addition, we found that a breach reported in the news media as having involved the National Park Service actually involved a not-for-profit organization that manages eParks, according to a representative of that organization. Four of the five breaches reported as having involved federal agencies were not believed to have resulted in identity theft, according to officials of the entities involved. The breach at

[38] *In the Matter of BJ's Wholesale Club, Inc.*, F.T.C. No. 0423160 (2005). A consent agreement does not constitute an admission of a violation of law.

FDIC resulted in an estimated 27 cases of identity theft when data inappropriately accessed by a former FDIC intern were used to take out more than $425,000 in fraudulent loans in the names of FDIC employees, according to agency officials.[39]

Industry and trade associations representing entities that maintain large amounts of information—banks, retailers, colleges, information resellers, and hospitals—told us that they had limited knowledge about the harm caused by data breaches that occur in their industries. However, in some cases, they provided information or anecdotal evidence on the extent to which such breaches may have led to some form of identity theft. For example, the 46 hospitals that the American Hospital Association surveyed at our request reported that of 17 breaches that had occurred since 2003, three had resulted in fraudulent activity on existing accounts and another three resulted in other forms of identity theft, including one case where the information was used to file false income tax refunds. The identity theft in these cases involved small numbers of victims—usually just one.

Representatives of the American Council on Education and two other higher education associations stated that while data breaches at colleges and universities were not uncommon, they were aware of little to no identity theft that had resulted from such breaches. Representatives of the American Bankers Association, the National Retail Federation, and the Consumer Data Industry Association told us they were unable to determine how prevalent data breaches are among their institutions or how often such breaches lead to consumer harm. Representatives at the National Retail Federation noted that breaches at retailers may be more likely to result in fraud on existing accounts than in new account creation, since most retailers do not maintain the personally identifiable information needed to steal someone's identity.

[39]According to an FDIC representative, the agency took several steps to address the possible misuse of employee information, including promptly notifying affected employees and offering them 2 years of credit monitoring services.

Of 24 Large Publicly Reported Breaches, 4 Apparently Resulted in Known Cases of Identity Theft

Using lists of data breaches compiled by the Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service, we identified the 24 largest breaches (measured by number of records) that were reported in the news media from January 2000 through June 2005.[40] To gather information on these incidents, we interviewed or collected written responses from representatives of the entity experiencing the breach and reviewed publicly available information, such as media reports, news releases, testimonies, and court documents. In some cases, when feasible, we also spoke with law enforcement investigators. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts.

Although these lists characterized each of these 24 incidents as data breaches, the circumstances of the incidents varied. While 19 of the incidents clearly met our definition of data breach (i.e. unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information), four cases involved hackers who may or may not have actually accessed sensitive information. In one other incident, a university employee with access to sensitive personal data was indicted on unrelated fraud charges. A university official told us he did not believe this incident should necessarily be characterized as a data breach since there was no evidence the employee actually misused university data.

The available evidence that we reviewed indicated that 18 of these 24 breaches were not known to have resulted in any identity theft. As shown in table 1, three breaches were believed to have resulted in account fraud and one resulted in the unauthorized creation of new accounts. In two

[40]These three organizations periodically update their lists by adding breaches they learn about that occurred in the past, including some that occurred between January 2000 and June 2005. Our list of the 24 largest media-reported breaches was based on information provided by these lists as of August 2006. We were not aware of the Attrition list at the time we made our selection. See Congressional Research Service, *Personal Data Security Breaches: Context and Incident Summaries*, Order Code RL33199 (Washington, D.C.: Dec. 16, 2005). Because our time frame covered only breaches that occurred on or before June 30, 2005, our list does not include highly publicized breaches that occurred subsequently, such as those involving the Department of Veterans Affairs and the TJX Companies. Several banks have reported fraudulent transactions on existing accounts resulting from the TJX breach, according to a January 24, 2007, press release by the Massachusetts Bankers Association.

other cases, we were not able to gather sufficient information on whether harm appeared to have resulted from the breach. Further, because of the challenges in linking data breaches with identity theft, in some cases our review may not have uncovered instances of harm potentially resulting from these breaches. In some instances, investigators or company representatives reported that they were able to determine with a high degree of certainty—through forensic investigation or other means—that unauthorized parties had not accessed the data. In other instances, these representatives said that they were not aware of any account fraud that resulted, but they acknowledged that there was no way to know for sure. Moreover, determining potential harm may be particularly challenging with very large breaches because the volume of records involved can make it difficult to link individual victims to the breach.

Table 1: Twenty-Four Large Publicly Reported Data Breaches and Evidence of Resulting Identity Theft, January 2000 - June 2005

The fact that we did not identify evidence of identity theft from a breach does not necessarily mean that no such harm has occurred or will occur in the future.

Year[a]	Type of organization	Nature of breach	Available evidence of identity theft?[b]
2000	Retail	Hacking	Account fraud
2000	Retail	Hacking	None identified
2002	Healthcare	Stolen computer equipment	None identified
2003	Higher education	Stolen computer equipment	None identified
2004	Financial services	Stolen computer equipment	None identified
2004	Higher education	Hacking	None identified
2004	Higher education	Hacking	None identified
2004	Higher education	Hacking	None identified
2004	Financial services	Lost data tapes	None identified
2005	Financial services	Hacking	Account fraud
2005	State government	Hacking	None identified
2005	Information services	Deception/Misrepresentation	Unauthorized new accounts
2005	Higher education	Hacking	None identified
2005	Higher education	Stolen computer equipment	None identified
2005	Retail	Hacking	Account fraud
2005	Information services	Deception/Misrepresentation	Unknown
2005	Healthcare	Stolen computer equipment	None identified
2005	Retail	Hacking	Unknown
2005	Financial services	Lost data tapes	None identified
2005	Financial services	Employee crime	None identified
2005	State government	Hacking	None identified
2005	Media	Lost data tapes	None identified
2005	Financial services	Lost data tapes	None identified
2005	Higher education	Other[c]	None identified

Source: GAO.

Note: To identify the 24 largest data breaches reported in the news media from January 2000 through June 2005, GAO analyzed lists of such breaches maintained by Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service.

[a]Year breach occurred or was publicized.

[b]The presence or lack of evidence of identity theft resulting from a breach was based on our review of news reports and other publicly available information, as well as interviews, as feasible, with representatives of entities experiencing the breach and law enforcement officials investigating the breach. The fact that we were unable to identify evidence at this time of identity theft resulting from a breach does not mean that no such harm has occurred or that none will occur in the future. Further, factual determinations of the existence and cause of identity theft in any particular case are matters for the courts to decide.

[c]In this case, a former university employee with access to sensitive personal information had been indicted on bank fraud charges unrelated to the university. Some press reports characterized this as a breach, but according to a representative of the university, there is no evidence that the employee misused university data.

The one large breach we identified that apparently resulted in the unauthorized creation of new accounts involved ChoicePoint, an information reseller. In 2005, the company acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services. FTC reached a civil settlement in 2006 with the company that established a fund for consumer redress to reimburse potential victims of identity theft, and the agency has worked with law enforcement officials to identify such victims.[41]

The three large breaches we identified that appeared to result in fraud on existing accounts included the following:

- CardSystems, a credit card payment processor, reported a May 2005 breach in which a hacker accessed data such as names, card account numbers, and expiration dates. The total number of compromised accounts is unclear. FTC staff alleged in a 2006 civil complaint that the breach had compromised data associated with tens of millions of credit and debit cards, but a CardSystems official stated in congressional testimony that only 239,000 accounts were compromised. Officials of the Office of the Comptroller of the Currency—who surveyed the national banks they supervise in order to determine the amount of fraudulent charges that resulted from the breach—said that customers of 110 banks were affected by this incident and losses of more than $13

[41]*United States v. ChoicePoint, Inc.*, No. 1:06-cv-00198-JTC (N.D. Ga., Feb. 15, 2006). As part of the settlement, ChoicePoint admitted no violations of the law. According to ChoicePoint, the company has subsequently taken steps to enhance its customer screening process and to assist affected consumers. FTC staff told us that law enforcement officials have determined that as many as 2,900 people have experienced the fraudulent creation of new accounts as a result of the breach. According to a ChoicePoint official, the criminal indictments indicated that 46 people may have been defrauded, but the accused individuals may not have used data acquired from ChoicePoint in all the crimes cited in the indictments.

million in fraudulent charges on customers' cards were reported by 24 of these institutions.

- DSW, a shoe retailer, said in an April 2005 news release that it had experienced a data breach in which a hacker accessed the names and card numbers associated with 1.4 million credit and debit card transactions at 108 of its stores, as well as checking account numbers and driver's license numbers from 96,000 check transactions. According to a complaint filed by FTC in March of 2006, there allegedly have been fraudulent transactions on some of these accounts.

- CD Universe, an Internet-based music store, reportedly experienced a breach in December 1999 in which a hacker accessed as many as 300,000 names, addresses, and credit card numbers from the company Web site, according to media reports and a company official. The hacker allegedly used some of the stolen credit card numbers to obtain money for himself.[42]

Challenges Exist in Determining the Link between Data Breaches and Identity Theft

Determining the link between data breaches and identity theft is challenging for several reasons. First, identity theft victims often do not know how their personal information was obtained. According to FTC, in approximately 65 percent of the identity theft complaints it received from October 1, 2005, through August 31, 2006, the victim did not know or report how the information was compromised. Second, victims may misattribute how their data were obtained. For example, federal officials and representatives of a private group that assists victims said that consumers who are notified of a breach often assume that any perceived mistakes on their credit card statements or credit report were a result of the breach. As a result, no government agency maintains comprehensive data on the underlying cause of identity theft. FTC told us that its Identity Theft Data Clearinghouse is limited to self-reported complaints and therefore does not contain statistically reliable information that would allow the agency to determine a link between data breaches and identity theft. Similarly, according to FBI, data maintained by the Internet Crime Complaint Center does not include information sufficient to determine the link between data breaches and identity theft.

[42]This breach occurred in December 1999 but was included in the 24 breaches we reviewed because it was reported in the media in January 2000.

Third, law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. Finally, conducting comprehensive studies of data breaches and identity theft can be hindered by issues of privacy and confidentiality. For example, companies that have experienced breaches may be unable or unwilling to provide information about affected individuals to researchers.

Some studies conducted by private researchers have sought to determine the extent to which data breaches result in identity theft, but our review found them to contain methodological limitations.[43] One research firm conducted a study of four data breaches, analyzing credit and other application data for suspicious relationships that indicated fraud.[44] The study estimated that no more than 0.10 percent of individuals whose data had been breached experienced resulting identity theft in the form of unauthorized new account creation. However, because the study reviewed only four data breaches, it cannot be considered representative of other breaches. Moreover, two of these breaches did not involve personally identifiable information and thus would not be expected to create a risk of fraud involving new account creation.

Another private research firm surveyed approximately 9,000 individuals about whether they had ever received a notification from an organization about the loss or theft of their personal information.[45] Of the approximately 12 percent of individuals who reported they had received such a notification, 3 percent—or 33 people—said they believed they had suffered identity theft as a result. However, these data are subject to limitations; among other things, individuals are often unaware of whether any fraud they have suffered was, in fact, due to a data breach. A third firm projected in a study that 0.8 percent of consumers whose information a

[43]Although we found limitations in how these studies linked data breaches and identity theft, we determined other aspects of these studies to be sufficiently reliable, and we refer to them elsewhere in this report.

[44]ID Analytics, Inc., *National Data Breach Analysis* (2006).

[45]Ponemon Institute, *National Survey* (2005). As noted earlier, this study may also be limited by a low survey response rate.

data breach compromised would experience fraud as a result.[46] However, we question the reliability of this estimate, in part because of assumptions made about the number of consumers affected by data breaches.

Type of Data Compromised and Other Factors Influence Potential for Resulting Consumer Harm

The type of data compromised in a breach can effectively determine the potential harm that can result. For example, credit or debit card information such as card numbers and expiration dates generally cannot be used alone to open unauthorized new accounts. Some of the largest and most highly publicized data breaches in recent years largely involved credit or debit card data rather than personally identifiable information. As a result, these breaches put affected consumers at risk of account fraud but not necessarily at risk of fraud involving unauthorized creation of new accounts—the type of identity theft generally considered to have a more harmful direct effect on consumers. While credit and debit card fraud is a significant problem—the FTC estimates it results in billions of dollars in losses annually—existing laws limit consumer liability for such fraud and, as a matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges.[47] In contrast, the unauthorized creation of new accounts—such as using someone else's identity to open credit card or bank accounts, originate home mortgages, file tax returns, or apply for government benefits—can result in substantial financial costs and other hardships.

In addition to the type of data compromised in a breach, several additional factors can influence the extent to which a breach presents the risk of identity theft. These include the following:

- *Intent.* Breaches that are the result of intentional acts—such as hacking into a server to obtain sensitive data—generally are considered to pose more risk than accidental breaches such as a lost laptop or the

[46]Javelin Strategy & Research, *Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses* (Pleasanton, California, August 2006).

[47]For unauthorized credit card charges, consumer liability is limited to a maximum of $50 per account, 15 U.S.C. § 1643. For unauthorized ATM or debit card transactions, the Electronic Fund Transfer Act limits consumer liability, depending on how quickly the consumer reports the loss or theft of the card. Pub. L. No. 90-321, tit. IX, as added Pub. L. No. 95-630, tit. XX, § 2001, 92 Stat. 3728 (Nov. 10, 1978); 15 U.S.C. § 1693g. Consumers may incur additional costs if they inadvertently pay charges they did not incur. In addition, account fraud can cause inconvenience or temporary hardship—such as losing temporary access to account funds or requiring the cancellation and reactivation of cards and the redirecting of automatic payments and deposits.

unintentional exposure of sensitive data on the Internet, according to federal agency officials. However, in some cases, such as the theft of a laptop containing personal information, it may be unknown whether the laptop was stolen for the hardware, the personal data, or both.

- *Encryption*. Encryption—encoding data so that it can only be read by authorized individuals—can in some cases prevent unauthorized access. However, some forms of encryption are more effective than others, and encryption does not necessarily preclude fraudulent use of data—for example, if the key used to unencrypt the data is also compromised.

- *Hardware requirements*. Data that only can be accessed using specialized equipment and software may be less likely to be misused in the case of a breach. For example, some entities that have lost data tapes have stated that criminals would require specific data reading equipment and expertise in how to use it to access the information.

- *Number of records*. Larger breaches may pose a greater overall risk that at least one individual would become a victim of identity theft. At the same time, given the resources needed to commit identity theft, breaches of very large numbers of records may pose less risk to any one individual whose data were compromised.

Breach Notification Requirements Can Serve to Encourage Better Data Security Practices and Alert Consumers, but They Also Present Costs and Challenges

Breach notification requirements have several potential benefits, including creating incentives for entities to improve their data security practices (and thus prevent potential breaches from occurring), allowing affected consumers to take measures to prevent or mitigate identity theft, and serving to respect individuals' basic right to know when their personal information is compromised. At the same time, breach notification requirements present costs, both for developing compliance strategies and for actual notifications in the event of a breach. Further, there is the risk of overnotification, or inundating consumers with frequent notifications of breaches that may present little or no risk of identity theft or other harm. Thus, policymakers face the challenge of setting a notification standard that allows individuals to take steps to protect themselves where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action.

Notification Requirements May Create Incentives for Improved Data Security and Allow Consumers the Opportunity to Mitigate Risks

According to our review of studies and interviews with representatives in government, academia, and private industry, breach notification requirements have several potential benefits, as follows:

- *Incentives for Improved Data Security*. Breach notification requirements can provide an incentive for companies and other entities to increase their data security measures to avoid the possible financial and reputational risks that can be associated with a publicly reported data breach.[48] Representatives we contacted in the private, nonprofit, and government sectors told us that they believe that existing breach notification requirements in state laws, or the breach notification provisions in federal banking regulatory guidance, have provided entities with incentives to improve data security practices. For example, some representatives of companies and other organizations noted that passage of state notification laws led to companies reexamining data security procedures and making improvements, such as encrypting sensitive data and restricting consumer data that can be accessed online. Similarly, federal banking regulators told us that they believe their notification guidance has motivated regulated institutions to enhance data security. For example, according to officials at the Office of Thrift Supervision, its institutions have taken steps such as improving electronic firewalls and implementing formal incident response reporting systems.

- *Prevention of Identity Theft*. Breach notification can provide consumers with the opportunity to take steps to protect themselves from possible identity theft. For example, consumers whose account information has been breached can monitor their bank or credit card statements for suspicious activity or close the affected accounts. Consumers whose personally identifiable information, such as SSN, has been breached can review their credit reports for suspicious activity or may choose to purchase a credit monitoring product that alerts them to changes that could indicate identity theft. In addition, affected consumers can place a fraud alert on their credit reports, which requires businesses to take certain identity verification steps before

[48]Such costs can be significant. For example, according to a 2006 survey, 31 companies that responded to the survey incurred an average of $98 per record, or $2.6 million per company, in costs associated with the loss of existing customers, recruitment of new customers, and damage to the reputation of their brand name. Ponemon Institute, LLC, *2006 Annual Study: Cost of a Data Breach*, 2006. Due to sampling limitations, these findings are not necessarily representative of the costs incurred by all companies that experience breaches.

issuing credit.[49] In some states, consumers can implement credit freezes, which block unauthorized third parties from obtaining the consumer's credit report or score.[50] Limited information exists on the steps individuals actually take when notified of a breach. In the 2005 Ponemon Institute survey of individuals that received notification letters, 50 percent said they did nothing, while the rest indicated they took actions such as monitoring their credit reports, canceling credit or debit cards, or closing bank accounts.[51]

- *Respecting Consumers' Right to Know*. Some consumer advocates and others have argued that consumers have a right to know how their information is being handled. According to this view, basic rights of privacy dictate that consumers should be informed when their personal information has been compromised, even if the risk of harm is minimal. The principle that individuals should have ready means of learning about the use of their personal information is embedded in the Fair Information Practices, a set of internationally recognized privacy protection principles.[52]

- *Improving Public Awareness*. Public reporting of data breaches may raise general awareness among consumers about the risks of identity theft and ways they can mitigate these risks, such as periodically reviewing their credit reports. In addition, publicity surrounding a data breach resulting from notification can serve to deter the use of stolen information because presumably the thief knows that the breach is likely being investigated and the stolen data are being carefully monitored.

[49]*See* 15 U.S.C. § 1681c-1.

[50]Congressional Research Service, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills* (Washington, D.C.: Jan. 11, 2007).

[51]Ponemon Institute, *National Survey* (2005). As noted earlier, this study may be limited by a low survey response rate.

[52]The Fair Information Practices were first proposed in 1973 by a U.S. government advisory committee. A revised version was developed in 1980 by the Organization for Economic Cooperation and Development, a group of 30 member countries that are market democracies. For more information, see GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

Breach Notification Requirements Present a Variety of Potential Costs

According to company representatives, researchers, regulators, and others, there are several different types of costs that may be associated with breach notification requirements. To begin with, entities subject to breach notification requirements may incur certain costs, regardless of whether they actually suffer a breach, or—if they do—regardless of whether they have to notify consumers. For example, entities may incur costs for developing and formalizing incident response plans.

There are also the costs associated with actual notifications—potentially including printing, postage, legal, investigative, and public relations expenses.[53] Although comprehensive data on these costs do not exist, a 2006 Ponemon Institute survey of companies experiencing a data breach found that 31 companies that responded incurred an average of $1.4 million per breach, or $54 per record breached, for costs related to mailing notification letters, call center expenses, courtesy discounts or services, and legal fees.[54] Similarly, a study by Gartner Research found that ChoicePoint spent $79 per affected account following its 2005 breach for professional fees, legal expenses, and communications to affected customers.[55] A representative of the San Jose Medical Group told us it spent $100,000 to send notification letters to 187,000 patients following a data breach that occurred in 2005. Entities also may incur costs related to staffing call centers to field inquiries from consumers about the breach. For example, representatives of the University of California at Berkeley told us that following a 2005 breach of 98,000 records, the university spent $75,000 in staffing, telecommunications, and other call center costs.

Finally, banks whose customers' account information is breached also may incur costs for remedial steps such as canceling existing accounts or replacing affected customers' credit or debit cards—although such steps may not be required by the applicable breach notification requirements.

[53]The distinction between the costs associated with a notification requirement versus a breach itself can be ambiguous. For example, the cost of postage can clearly be attributed to notification, whereas legal costs can be attributed to notification, the breach itself, or both, depending on the circumstances.

[54]Ponemon Institute, *Annual Study* (2006). As noted earlier, due to sampling limitations, these findings are not necessarily representative of the costs incurred by all companies that experience breaches.

[55]Gartner Research, *Data Protection Is Less Costly Than Data Breaches* (Stamford, Connecticut: September 16, 2005). The report, issued in 2005, based its findings on the breach having affected 145,000 records, but company officials later reported that 162,000 records were affected.

Entities experiencing a breach also often provide affected individuals with free credit monitoring services. For example, a representative of a large financial management company noted that offering free credit monitoring services after a breach has become standard industry practice, and costs, on average, between $20 and $40 per customer.

Challenges Exist in Complying with and Developing Breach Notification Requirements

Officials of companies and other entities we interviewed identified challenges such as interpreting ambiguous statutory language, identifying and locating affected consumers, and developing effective notification letters. In addition, policymakers face challenges in developing breach notification requirements, particularly in setting the appropriate standard to establish the circumstances under which consumers should be notified.

Complying with Notification Requirements

Companies and other entities we interviewed said they can face a number of challenges related to complying with the breach notification requirements in state laws or federal banking guidance. These include the following:

- *Interpreting ambiguous provisions.* Entities subject to breach notification requirements sometimes face challenges interpreting certain terms or provisions of notification laws. For example, an information security expert told us that some laws do not adequately define encryption, which could refer to anything from simple password protection to complex coding. Similarly, federal banking regulators acknowledged that their institutions sometimes face difficulty determining whether misuse of breached information is "reasonably possible," such as when little information exists about the location of the data, the intent of a criminal who stole data, or the effectiveness of security features designed to render data inaccessible.

- *Addressing who is responsible.* Notification requirements do not always fully address who should bear the cost of and responsibility for notification, particularly in cases where a third party is responsible for the breach. For example, representatives of some federal banking regulators and industry associations cited particular challenges associated with breaches of credit and debit card information by retailers. Banks that issue credit and debit cards compromised by a merchant that is not the bank's service provider are generally not required by the banking regulators' guidance to notify their customers, but nevertheless in some cases, they feel obliged to do so. Bank representatives with whom we spoke expressed concern that breaches of credit card information by third parties can adversely affect a bank's

reputation and result in costs related to notifying customers and reissuing cards.

- *Identifying affected consumers*. Some entities we interviewed said that it can be difficult to identify which consumers may have been affected by a breach and obtain their contact information. For example, one representative at a state agency involved in a breach told us officials were unsure what data had been downloaded among records that may have been accessed on 600,000 people. Obtaining accurate and current mailing addresses for affected parties also can be difficult and costly, many entities told us. This can be a particular problem for entities, such as merchants, that have breached credit card numbers but do not themselves possess the mailing addresses associated with those numbers.

- *Developing clear and effective notification letters*. We have noted in the past that public notices should be useful and easy to understand if they are to be effective.[56] However, the 2005 study conducted by the Ponemon Institute found that 52 percent of survey respondents who received a notification letter said the letter was not easy to understand.[57] In addition, consumers might be confused by other mail solicitations that may resemble notification letters. For example, officials at one large national bank noted that marketing solicitations for credit monitoring services often are made to resemble breach notification letters, potentially desensitizing or confusing consumers when a true notification letter arrives.

- *Complying with multiple state laws*. Officials of companies with customers in multiple states and their trade associations noted that they face the challenge of complying with breach notification requirements that vary among the states, including who must be notified, the level of risk that triggers a notice, the nature of the notification, and exceptions to the requirement. Officials of companies we contacted noted that it is challenging to comply with these multiple requirements since most breaches involve customers in many states.

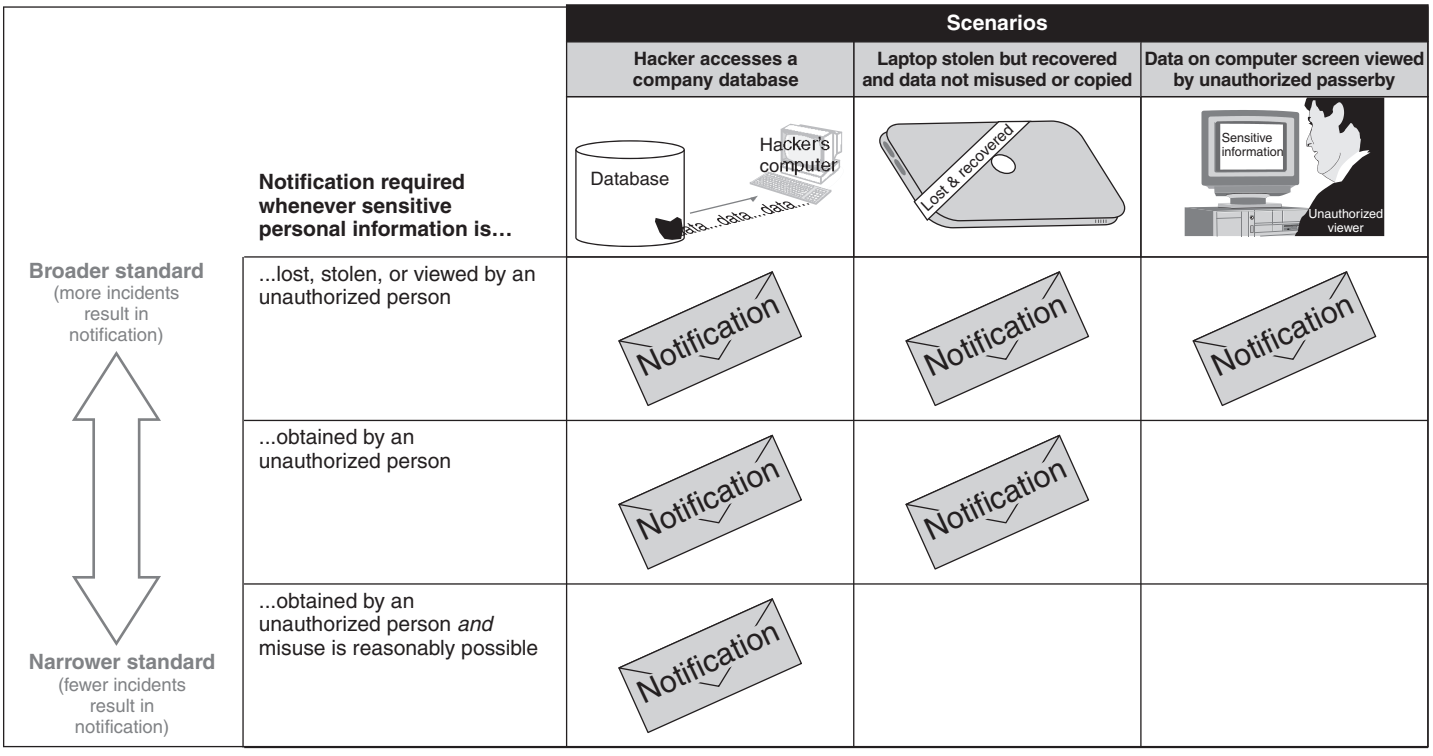
[56]*See* GAO-06-833T, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information* (Washington, D.C.: Jun. 8, 2006), pp. 15-18, which discusses specific elements that should be incorporated in a breach notification.

[57]Ponemon Institute, *National Survey* (2005). As noted earlier, this study may be limited by a low survey response rate.

Setting an Appropriate Notification Standard

Existing state laws vary in terms of the notification standard—that is, the event or circumstance that triggers a required notification. For example, California has an expansive standard that requires notification in nearly all cases where unencrypted sensitive personal data "is reasonably believed to have been acquired by an unauthorized individual." Other states employ a risk-based approach that incorporates into the standard the extent to which the data are likely to be misused. The standards vary in terms of what is required in cases where the risk of harm is unknown. For example, Vermont requires notification unless an entity can demonstrate that misuse of the breached data "is not reasonably possible." In contrast, North Carolina requires notification only when it has been determined that the breach has resulted, or is reasonably likely to result, in illegal use of the data or creates a material risk of harm to a consumer. As shown in figure 1, whether or not a breach is subject to notification can depend on the specific notification standard.

Figure 1: Application of Notification Standards under Different Breach Scenarios



Source: GAO (analysis); Art Explosion (images).

Note: Figure presents hypothetical scenarios and notification standards and is shown for illustrative purposes only.

Because of the difficulty of complying with multiple state requirements, many companies and industry representatives have argued for a consistent federal standard for breach notification that would preempt state notification laws. However, the National Association of Attorneys General, as well as some consumer and privacy groups, have expressed concern that a federal breach notification law could weaken consumer protections if it were to preempt stronger state laws. These groups have advocated a strong notification standard because, they say, the link between breaches and identity theft is not always clear and entities are not well equipped to assess the risk of harm resulting from a given breach. As a result, too narrow a notification standard may prevent consumers from taking action in cases that do in fact present some risk. Also, as noted earlier, some privacy groups and others believe that consumers have basic rights to be notified when their personal information has been breached, no matter what the circumstances. Moreover, they say that fears of "overnotification"—where consumers are inundated by frequent notifications—are unfounded, given that they are aware of no evidence of this occurring in states that currently have strict notification requirements.

By contrast, some representatives of the federal banking regulatory agencies, FTC, private companies, and other experts have expressed concern about overly expansive breach notification standards. They say that such standards may require businesses to notify consumers about minor and insignificant breaches. This in turn could eventually lead to overnotification and cause consumers to spend time and money taking proactive steps that are not necessary or, alternatively, to ignore notices when action is warranted. In addition, businesses and federal banking regulators have expressed concern about the financial burden that overnotification could cause. Overly broad notification standards could also have the effect of limiting entities' reputational incentives for improving data security, if nearly all entities regularly issue notifications as a result of minor breaches. Representatives of the federal banking regulatory agencies have noted that they sought to strike an appropriate balance with their notification standard. Their guidance provides that, when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.[58] If the institution determines that

[58]12 C.F.R. Pt. 30, App. B, Supp. A § III(A); 12 C.F.R. Pt. 208, App. D-2, Supp. A § III(A); 12 C.F.R. Pt. 225, App. F, Supp. A § III(A); 12 C.F.R. Pt. 364, App. B, Supp. A § III(A); 12 C.F.R. Pt. 570, App. B, Supp. A § III(A); and 12 C.F.R. Pt. 748, App. B § III(A).

misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible. The guidance is intended to provide notice to customers only when there is a reasonable expectation of misuse.[59]

Similarly, the guidance for federal agencies developed by the President's Identity Theft Task Force recommended that if an agency experiences a breach, it should analyze the risk of identity theft and tailor its response—which may include notifying individuals—to the nature and scope of the risk presented. The guidance noted that such a risk assessment can minimize the potentially significant costs of notification where little risk exists. The task force's April 2007 strategic plan recommended the development of a national standard requiring all entities that maintain sensitive consumer information, in both the public and private sectors, to provide notice to consumers and law enforcement in the event of a breach. As with its guidance to federal agencies, the task force recommended that the standard be risk based to provide notice when consumers face a significant risk of identity theft but to avoid excessive notification.

As we have noted in the past, care is needed in defining appropriate criteria for data breaches that merit notification.[60] The frequency of data breaches identified in this report suggests that a national breach notification requirement may be beneficial, in large part because of its role in further encouraging entities to improve their data security practices. However, because breaches vary in the risk they present, and because most breaches have not resulted in detected incidents of identity theft, a notification that is risk based appears appropriate. Should Congress choose to enact a federal breach notification requirement, use of the risk-based approaches that the federal banking regulators and the President's

[59]The guidance states that institutions should notify their primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, even for incidents that may not warrant customer notification. Banking regulators told us they review institutions' response programs as part of their supervisory procedures and, in many cases, work with institutions as they respond to specific incidents to ensure their actions are in accordance with the guidance. *See* 12 C.F.R. Pt. 30, App. B, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 208, App. D-2, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 225, App. F, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 364, App. B, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 570, App. B, Supp. A § II(A)(1)(b); and 12 C.F.R. Pt. 748, App. B § II(A)(1)(b).

[60]GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: Jun. 26, 2006) and GAO-06-833T.

Identity Theft Task Force advocate could avoid undue burden on organizations and unnecessary and counterproductive notifications to consumers.

Agency Comments

We provided a draft of this report to FTC, which provided technical comments that were incorporated in this report as appropriate. In addition, we provided selected portions of the draft to the Board of Governors of the Federal Reserve System, the Department of Justice, DHS, FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Social Security Administration, and USPIS, and also incorporated their technical comments as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Chairman, House Committee on Financial Services; the Chairman and Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Member, Senate Committee on the Judiciary; the Chairman and Ranking Member, House Committee on the Judiciary; the Chairman and Vice Chairman, Senate Committee on Commerce, Science, and Transportation; and the Chairman and Ranking Member, House Committee on Energy and Commerce. We will also send copies to the Chairman of the Board of Governors of the Federal Reserve System, the Attorney General, the Secretary of the Department of Homeland Security, the Chairman of the Federal Deposit Insurance Corporation, the Chairman of the Federal Trade Commission, the Chairman of the National Credit Union Administration, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Commissioner of the Social Security Administration, and the Postmaster General and Chief Executive Officer of the U.S. Postal Service. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or woodd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

David G. Wood
Director, Financial Markets and
Community Investment

Appendix I: Scope and Methodology

Our report objectives were to examine (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. We use the term "data breach" to refer to the unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information by a company, government agency, university, or other public or private entity. Our scope was limited to breaches involving personal data, including financial data, that could be used to commit identity theft or other related harm, and we excluded breaches involving other types of sensitive data, such as medical records or proprietary business information. For the purposes of this report, the term "identity theft" is used broadly to refer to both fraud on existing accounts and the unauthorized creation of new accounts.

To address all three objectives, we conducted a literature search of relevant articles, reports, and studies. We also collected and analyzed documents from, and interviewed, officials of government agencies that investigate and track data breaches, including the Federal Trade Commission, the Department of Homeland Security, the Department of Justice, the U.S. Postal Inspection Service, and the Social Security Administration. We also interviewed staff at the five federal banking regulators—the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration. In addition, we spoke with representatives of the National Association of Attorneys General and organizations that address consumer protection and privacy issues, including Consumers Union, Electronic Privacy Information Center, Privacy Rights Clearinghouse, Attrition, and the Identity Theft Resource Center. We also spoke with three academic researchers who study issues related to data breaches and notification and an attorney who helps companies address data privacy and security issues. In addition, we reviewed studies on data breaches conducted by private and nonprofit research organizations, including the Ponemon Institute, ID Analytics, and Javelin Strategy and Research. We interviewed the studies' authors and took other steps to ensure that the data and methodologies were sufficiently reliable for our purposes. We also spoke with representatives of the California Office of Privacy Protection and its advisory group and reviewed the office's recommended practices for notification.

To address the first objective on the incidence and circumstances of data breaches, we reviewed lists of news media-reported data breaches that are compiled and maintained by three private research and advocacy organizations—Privacy Rights Clearinghouse, Attrition, and the Identity Theft Resource Center. We analyzed the three independent lists to create a single, nonduplicative list of data breaches that had been reported in the news media from January 2005 through December 2006. We took measures to ensure the lists were of sufficient quality for our purposes, including spot checking selected data and interviewing representatives of the three organizations on their methodologies. The Privacy Rights Clearinghouse, Attrition, and Identity Theft Resource Center lists contained 436, 453, and 462 breaches, respectively, for the time period we analyzed. Of the 572 breaches they collectively compiled, 59 percent appeared on all three lists, 19 percent appeared on two, and 22 percent appeared on one. Our analysis was based on the lists as they stood on February 15, 2007; these data may have changed because the lists are occasionally updated when the compilers learn of new breaches that may have occurred in the past.

We also collected available data from federal law enforcement agencies on the breaches they have investigated in recent years. In addition, the five federal banking regulators provided, at our request, data on the breaches of which they have been notified by the institutions they supervise. These data varied in usefulness and comprehensiveness because of the regulators' differing methods of counting and tracking breaches and maintaining data on them. We also gathered data from two states, New York and North Carolina, which were selected because they were two large states that maintain centralized information on breaches. Further, we obtained available data from industry and trade associations representing key sectors—such as financial services, retail sales, higher education, hospitals, and information services—that have experienced data breaches. We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee and the U.S. Computer Emergency Readiness Team, a component of the Department of Homeland Security.

To address the second objective, we selected for more detailed examination the 24 largest (in terms of number of records breached) data breaches reported in the news media from January 2000 through June 2005. We selected these breaches in August 2006 using the lists maintained by Privacy Rights Clearinghouse and Identity Theft Resource Center, as well as a similar compilation of breaches collected by the Congressional Research Service. We were not aware of the Attrition list at the time we

made our selection. For each of these breaches, we reviewed news reports as well as publicly available documents such as testimonies and criminal indictments. We also conducted interviews, where possible, with representatives of the entities that experienced the breach and law enforcement agencies that investigated the breach. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts. We did not directly contact individuals whose data had been affected by the breaches because of privacy concerns and because we did not have a systematic means of identifying them. We also reviewed five breaches that reportedly involved federal agencies—the Navy; the Internal Revenue Service; the Federal Deposit Insurance Corporation; the National Park Service; and the Department of Justice. These were selected to represent breaches that included different causes, types of data, and involvement by third-party vendors.

To examine the potential benefits, costs, and challenges associated with breach notification requirements, we reviewed the federal banking regulators' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law. We interviewed representatives of, and gathered information from, seven organizations to learn about their experiences complying with California's breach notification law. These organizations were selected to represent a range of organization sizes and industry sectors. We also interviewed representatives of the California State Information Security Office, California State Assembly, California Office of Privacy Protection, and California Bankers Association.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

David G. Wood, (202) 512-8678 or woodd@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jason Bromberg, Assistant Director; Randy Fasnacht; Marc Molino; Kathryn O'Dea; Carl Ramirez; Linda Rego; Barbara Roesmann; and Winnie Tsen made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548