Order Code RL33199

CRS Report for Congress
Received through the CRS Web

Data Security Breaches: Context and Incident Summaries

Updated September 28, 2006

Rita Tehan
Information Research Specialist
Knowledge Services Group

Data Security Breaches:
Context and Incident Summaries

Summary

Personal data security breaches are being reported with increasing regularity. Within the last few years, numerous examples of data such as Social Security numbers, bank account, credit card, driver's license numbers, and medical and student records have been compromised. A major reason for the increased awareness of these security breaches is a California law that requires notice of security breaches to the affected individuals. This law, implemented in July 2003, was the first of its kind in the nation.

State security breach notification laws require companies and other entities that have lost data to notify affected consumers. Over half the states considered security breach notice and security freeze legislation in 2005, and several states passed laws requiring that individuals be notified of security breaches.

Congress is considering legislation to address personal data security breaches, following a series of high-profile data security breaches at major financial services firms, data brokers (including ChoicePoint and LexisNexis), and universities. Multiple measures were introduced in 2005 and 2006, but to date, none have been enacted.

For a discussion of legislative and other issues on this topic, see

- CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens
- CRS Report RL33273, *Data Security: Federal Legislative Approaches*, by Gina Marie Stevens
- CRS Report RS22484, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, by Kristin Thornblad
- CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation in the 109th Congress, 1st Session*, by Marcia S. Smith;
- CRS Report RL33005, *Information Brokers: Federal and State Laws*, by Angie A. Welborn;
- and CRS Report RS22082, *Identity Theft: The Internet Connection*, by Marcia S. Smith.

This report will be updated regularly.

Contents

List of Tables

Data Security Breaches: Context and Incident Summaries

Introduction

Personal data security breaches are being reported with increasing regularity. During the past few years, there have been numerous examples of hackers breaking into corporate, government, academic, and personal computers and compromising computer systems or stealing personal data such as Social Security numbers, bank account, credit card, and driver's license numbers, and medical and student records. These breaches occur not only because of illegal or fraudulent attacks by computer hackers, but often because of careless business practices, such as lost or stolen laptops, or the inadvertent posting of personal data on public websites. A recent infamous example occurred in May 2006, when 26.5 million veterans and their spouses were in danger of identity theft because a Veterans Affairs data analyst took home a laptop containing personal data (including names, Social Security numbers, and dates of birth), which was later stolen in a burglary. For additional information on legislative proposals introduced after the VA data theft (and in light of several ongoing information security and information technology management issues at the VA), see CRS Report RL33612, *Department of Veterans Affairs: Information Security and Information Technology Management Reorganization*, by Sidath Viranga Panangala.

A California law that requires notice of security breaches to the affected individuals is the major reason for the increased awareness of these breaches.[1] This law, which was implemented in July 2003, was the first of its kind in the nation.

State security breach notification laws[2] require companies and other entities that have lost personal data to notify affected consumers. Over half the states considered

---

[1] California Department of Consumer Affairs, Office of Privacy Protection, *Notice of Security Breach - Civil Code Sections1798.29 and 1798.82 - 1798.84*, updated June 24, 2003, at [http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29], and [http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84] and *Recommended Practices on Notification of Security Breach Involving Personal Information*, Oct. 10, 2003, at [http://www.privacy.ca.gov/recommendations/secbreach.pdf].

[2] See also *2005 Breach of Information Legislation*, National Conference of State Legislatures at [http://www.ncsl.org/programs/lis/CIP/priv/breach.htm].

security breach notice and security freeze[3] legislation in 2005, and several states passed laws requiring that individuals be notified of security breaches.[4]

An estimated 10 million consumers are affected annually by lost or stolen data at a cost to the economy of $53 billion.[5] Moreover, victims spend almost 300 million hours a year trying to clear their names and re-establish good credit ratings.[6] For additional information on this, see CRS Report RL31919, *Remedies Available to Victims of Identity Theft*, by Angie Welborn.

Despite the growing fear of data security breaches, a new study suggests that consumers whose credit cards are lost or stolen or whose personal information is accidentally compromised face little risk of becoming victims of identity theft.[7] After six months of study, an analysis by ID Analytics, a fraud-detection company, found that different breaches pose different degrees of risk. In the research, ID Analytics distinguishes between "identity-level" breaches, where names and Social Security numbers are stolen and "account-level" breaches, where only account numbers — sometimes associated with names — are stolen. The report concludes that even in the most dangerous data breaches, where thieves access Social Security numbers and other sensitive information about consumers they have deliberately targeted, the fraud rate is 0.098% — less than one in 1,000 identities are potentially revealed.[8]

> While initially surprising, the seemingly low misuse rate recognizes a fundamental truth about identity fraud. It is the fraud ring's available resources that determine how much attempted misuse follows a targeted, identity-level data breach. Fraud rings simply do not have the time or manpower to use hundreds of

---

[3] A security freeze law allows a customer to block unauthorized third parties from obtaining his or her credit report or score. A consumer who places a security freeze on his or her credit report or score receives a personal identification number to gain access to credit information or to authorize the dissemination of credit information. Source: CRS Report RS22484, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*.

[4] In 2005, security breach notification legislation was introduced in at least 35 states. At least 22 states have enacted security breach notification laws, and a similar bill awaits gubernatorial action in New Jersey. Security breach notification laws have been enacted in the following states: AK, CA, CT, DE, FL, GA (data brokers only), IL, IN (state agencies only), LA, ME, MN, MT, NV, NJ, NY, NC, ND, OH, RI, TN, TX, WA. *State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, U.S. Public Interest Research Group (USPIRG) at [http://www.pirg.org/consumer/credit/statelaws.htm#breach]. See CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens.

[5] Federal Trade Commission, *Identity Theft Survey Report*, Sept. 2003, at [http://www.consumer.gov/idtheft/pdf/synovate_report.pdf].

[6] Peter Katel, "Identity Theft: Can Congress Give Americans Better Protection?," *CQ Researcher*, June 10, 2005.

[7] Reuters, "ID Theft Risk Lower in Large-Scale Security Breaches," Computerworld, Dec. 8, 2005, at [http://www.computerworld.com/printthis/2005/0,4814,106854,00.html].

[8] ID Analytics, "ID Analytics' First-Ever National Data Breach Analysis Shows the Rate of Misuse of Breached Identities May be Lower than Anticipated," press release, Dec. 8, 2005, at [http://www.idanalytics.com/news_and_events/20051208.htm].

> thousands of identities available to them in their nefarious pursuits. Think about this practically. If a fraudster spent five minutes to fill out a new account application that is likely to be approved, one application per unique identity, worked 6.5 hours per day, it would take that individual over 50 years to utilize a breached file of one million consumer identities. This scenario overlooks other practicalities, such as procuring the applications and the need to launder the proceeds over time. The misuse rate could increase drastically if the current black market for "identities" remains unimpeded and becomes more centralized and efficient.[9]

Crimes involving electronic data can be very labor intensive for the criminal. Account information may be stolen in bulk with a few efficient lines of software code, but it is sold in much smaller numbers to other criminals who withdraw money or buy goods one transaction at a time, and usually only for a short period until the fraudulent activity is detected.[10]

More than three-quarters of companies recently surveyed by Deloitte Touche Tohmatsu said they have suffered a security breach from the outside, up sharply from the 26% that said they have suffered one when polled in 2005. But even for companies, it is difficult to find specific examples where hacking (or other type of breaches, such as lost or stolen laptops or computers, or inadvertent posting of personal data to public websites) resulted in substantial financial losses. Businesses cite high costs associated with replacement of credit/debit cards, remediation outreach programs to notify people of security breaches, and efforts to protect against lawsuits by security breach victims. "Theft of information is out of control, but use of that information to commit fraud is not out of control," says Avivah Litan, senior analyst at Gartner Inc., a technology research firm. The truth is, in the great majority of cases involving consumers, criminals don't have enough data with which to commit a crime."[11]

In addition, an August 2006 study by the Elk Rapids, MI-based privacy management research company Ponemon Institute finds that only 37% of information technology professionals believe their company is effective at preventing data breaches.[12] Citing a lack of resources and high product costs as barriers to preventing data leakages, only 43% believed their company would detect a large data breach (involving more than 10,000 customer records) more than 80% of the time.[13]

---

[9] ID Analytics, "National Data Breach Analysis: Frequently Asked Questions," 2006 at [http://www.idanalytics.com/pdf/National_DataBreach_FAQ.pdf]

[10] Henry Fountain, "Worry. But Don't Stress Out," *New York Times*, June 26, 2005, sec. 4, p. 1.

[11] Dean Foust, "ID Theft: More Hype than Harm," *Business Week Online*, July 3, 2006, at [http://www.businessweek.com/magazine/content/06_27/b3991041.htm].

[12] Deborah Rothberg, "IT Pros Say They Can't Stop Data Breaches," eWeek, August 30, 2006 at [http://www.eweek.com/article2/0,1759,2010325,00.asp?kc=EWRSS03129TX1K0000614].

[13] Sponsored by Port Authority Technologies, independently conducted by Ponemon Institute, National Survey on the Detection and Prevention of Data Security Breaches, (continued...)

Moreover, according to a June 2005 survey by Gartner, Inc., nearly 60% of consumers say they worry more about thieves getting undetected access to private credit reports and other sensitive financial data than defending against phishing attacks.[14] Nearly one-third are "extremely concerned" that they will suffer some type of identity theft fraud because of unauthorized access to their data.[15]

A fraud specialist with Gartner, Inc., concludes that because the crime is often misclassified, identity thieves have a one out of 700 chance of being caught.[16] In other words, the risk to benefit ratio favors the criminal. "It's a crime in which you can get a lot of money and have a very low probability of ever getting caught," Mari J. Frank, a lawyer and author of several books on identity theft, said in a *New York Times* interview. "Criminals are now saying, Why am I using a gun?"[17]

The Identity Theft and Assumption Deterrence Act of 1998 established the Federal Trade Commission (FTC) as the government entity charged with developing "procedures to ... log and acknowledge the receipt of complaints by individuals," as well as educate and assist potential victims.[18,19] The FTC compiles annual reports and charts of aggregated statistics on these events, but does not identify which corporations, organizations, or other entities have been victims of security breaches.[20] The FTC is also an enforcement agency and does not release data on companies while an investigation is ongoing. At the completion of the investigation, when there is an enforcement action, the FTC then releases information identifying corporations, organization, or others who have violated data security laws.

---

[13] (...continued)
August 28, 2006, at
[http://www.portauthoritytech.com/resources/downloads/wp_Ponemon_Institute_Study.pdf]

[14] Phishing is e-mail fraud where the perpetrator sends out legitimate-looking e-mails that appear to come from well-known and trustworthy websites in an attempt to gather personal and financial information from the recipient.

[15] "Data Security Lapses, Increased Cyber Attacks Damage Consumer Trust in E-Commerce," *Government Technology*, June 27, 2005, at
[http://www.govtech.net/magazine/channel_story.php/94447].

[16] Avivah Litan, "Underreporting of Identity Theft Rewards the Thieves," Gartner, Inc., July 7, 2003.

[17] Tom Zeller, "For Victims, Repairing ID Theft Can be Grueling," *New York Times*, Oct. 1, 2005.

[18] Identity Theft and Assumption Deterrence Act, as amended by P.L. 105-318, 112 Stat. 3007 (Oct. 30, 1998), at [http://www.ftc.gov/os/statutes/itada/itadact.htm].

[19] For an overview of the federal laws that could assist victims of identity theft with purging inaccurate information from their credit records and removing unauthorized charges from credit accounts, as well as federal laws that impose criminal penalties on those who assume another person's identity through the use of fraudulent identification documents, see CRS Report RL31919, *Remedies Available to Victims of Identity Theft*, by Angie Welborn. (Relevant state laws are also discussed.)

[20] Federal Trade Commission, *ID Theft Data: State Data* website at [http://www.consumer.gov/idtheft/id_state.htm]. *National Data* is available at [http://www.consumer.gov/idtheft/id_federal.htm].

Although a number of federal agencies (e.g., the Federal Trade Commission, Department of Justice, Secret Service, U.S. Postal Service, and Social Security Administration), state attorneys general, and private organizations such as the Electronic Privacy Information Center are involved with data privacy investigations or related consumer assistance, none maintains a comprehensive itemized list of data security breaches.[21] However, the Privacy Rights Clearinghouse maintains a frequently-updated chronology of data breaches from February 2005 to the present.[22]

A number of data security breaches by federal agencies in recent months revealed many agencies do not have security controls in place (see **Table 3**: *Data Security Breaches in State and Federal Government*, below).[23] In the first half of 2006, the list of agencies with incidents of potentially compromised data include the Departments of Agriculture, Defense, Energy, Veterans Affairs, Transportation, the Federal Trade Commission, the Internal Revenue Service, the Government Accountability Office, the National Institutes of Health, and the Department of the Navy. The State Department also suffered a series of hacking attacks. In fiscal 2005, major federal agencies reported about 3,600 incidents that were serious enough to warrant alerting the government's cybersecurity center at the Department of Homeland Security, including 304 instances of unauthorized access and 1,806 cases of malicious computer code, according to a yearly OMB report.[24]

> [E]xperts say the federal government faces special challenges because of the variety of sensitive information it keeps, the increasingly mobile nature of the federal workforce and the pervasive use of contractors, which allow thousands of individuals with varying levels of security clearance to access government databases from remote sites. A 2004 government survey on the work practices of 1.8 million federal workers found that more than 140,000 had clearance to connect with government computer systems from home. The IRS says 50,000 of its employees have laptops allowing them to access personal and business tax information from anywhere. And 133 Education Department personnel can access more than 10,000 records containing student loan recipients' personal information.[25]

---

[21] For a brief discussion of federal and state data security laws, see CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens.

[22] Privacy Rights Clearinghouse, *A Chronology of Data Breaches* at [http://www.privacyrights.org/ar/ChronDataBreaches.htm]. The chronology "begins with ChoicePoint's 2/15/05 announcement of its data breaches because it was a watershed event in terms of disclosure to the affected individuals."

[23] Rebecca Adams, "Data Drip: How the Feds Handle Personal Data," *CQ Weekly*, July 10, 2006, p. 1846.

[24] Office of Management and Budget, *FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, March 1, 2006, at [http://www.whitehouse.gov/omb/inforeg/reports/2005_fisma_report_to_congress.pdf].

[25] Zachary Goldfarb, "To Agency Insiders, Cyber Thefts And Slow Response Are No Surprise," *Washington Post*, July 18, 2006, at [http://www.washingtonpost.com/wp-dyn/content/article/2006/07/17/AR2006071701170.html].

The United States Computer Emergency Readiness Team (US-CERT) has recently begun monitoring trends involving the acquisition of personally identifiable information (PII) by unauthorized, malicious users.[26]

On September 19, 2006, the President's Identity Theft Task Force adopted interim recommendations on measures that can be implemented immediately to help address the problem of identity theft. In a September 20, 2006 memo to federal department and agency heads[27], the Office of Management and Budget (OMB) outlined steps agencies should take in responding to an identity theft or ways to prevent one from happening. Clay Johnson, the Office of Management and Budget's deputy director for management, made it clear the administration supports the task force's recommendation that departments establish a "core management group responsible for responding to the loss of personal information..."[28]

The Identity Theft Task Force, which was established by Executive Order of the President on May 10, 2006[29], and is now comprised of 17 federal agencies and departments, is scheduled to deliver a final strategic plan to the President in November, 2006. The Identity Theft Task Force's interim recommendations to the Administration include the following:

- Data breach guidance to agencies
- Development of universal police report for identity theft victims
- Extending restitution for victims of identity theft
- Reducing access of identity thieves to Social Security Numbers
- Developing alternative methods of authenticating identities
- Improving data security in the government
- Improving agencies' ability to respond to data breaches in the government.[30]

In June, 2006, the Office of Management and Budget issued new security guidelines requiring federal civilian agencies to implement new measures to protect

---

[26] US-CERT, *Quarterly Trends and Analysis Report*, September 1, 2006, at [http://www.us-cert.gov/press_room/trendsandanalysisQ306.pdf]. This report summarizes and provides analysis of incident reports submitted to US-CERT during the third quarter of FY2006 (April 1, 2006 to June 30th, 2006).

[27] Office of Management and Budget Memorandum for the Heads of Departments and Agencies,*Recommendations for Identity Theft Related Data Breach Notification*, September 20, 2006, at
[http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf]

[28] Jason Miller, "OMB Issues Data Breach Guidance," Government Computer News, September 22, 2006, at [http://www.gcn.com/online/vol1_no1/42106-1.html].

[29] Executive Order 13402: *Strengthening Federal Efforts to Protect Against Identity Theft*, May 10, 2006, at [http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html].

[30] U.S. Department of Justice press release, *Identity Theft Task Force Announces Interim Recommendations*, September 19, 2006, at
[http://www.usdoj.gov/opa/pr/2006/September/06_ag_635.html].

the security of personal information held by federal agencies.[31] To comply with the new policy, agencies will have to encrypt all data on laptop or handheld computers unless the data are classified as "non-sensitive" by an agency's deputy director. Agency employees also would need two-factor authentication -- a password plus a physical device such as a key card -- to reach a work database through a remote connection, which must be automatically severed after 30 minutes of inactivity.[32]

In June 2006, a group of government agencies, corporations, and universities launched a research center dedicated to the study of identity fraud. The Center for Identity Management and Information Protection is dedicated to furthering a national research agenda on identity management, information sharing, and data protection.[33]

Congress is considering legislation to address data security, following a series of high-profile data security breaches at major financial services firms and data brokers, including ChoicePoint and LexisNexis. Multiple measures were introduced in 2005 and 2006, and several have been reported out of committee, but to date, none have been brought to the floor.

For a discussion of legislative and other issues on this topic, see

- CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens
- CRS Report RL33273, *Data Security: Federal Legislative Approaches*, by Gina Marie Stevens
- CRS Report RS22484, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, by Kristin Thornblad
- CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation in the 109th Congress, 1st Session*, by Marcia S. Smith;
- CRS Report RL33005, *Information Brokers: Federal and State Laws*, by Angie A. Welborn;
- and CRS Report RS22082, *Identity Theft: The Internet Connection*, by Marcia S. Smith.

Tables 1-5 summarize selected data security or identity theft breaches reported in the press since 2000. A few highlights compiled from the reported incidents:

- Almost half of the security breaches occurred at institutions of higher education. (A *Chronicle of Higher Education* article examines why this is so, noting that while colleges have become better at detecting electronic break-ins, security practices,

---

[31] Office of Management and Budget Memorandum for the Heads of Departments and Agencies, *Protection of Sensitive Agency Information*, June 23, 2006, at [http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf].

[32] Brian Krebs, "OMB Sets Guidelines for Federal Employee Laptop Security," *Washington Post*, June 27, 2006, at [http://www.washingtonpost.com/wp-dyn/content/article/2006/06/27/AR2006062700540.html]

[33] Center for Identity Management and Information Protection, at [http://www.utica.edu/academic/institutes/cimip/]

particularly password protections, are lax.[34] In addition, academic culture embraces the open exchange of information and provides a target-rich environment for data breaches — an abundance of computer equipment filled with sensitive data and a pool of financially naive students.[35]). In September 2006, Louisiana State University (LSU), under a year-long agreement with Equifax Inc., will provide students, faculty and staff members with free daily monitoring of their credit reports and $2,500 in identity-theft insurance. LSU claims this is the first agreement of its kind between a credit agency and a higher-education institution. The university will pay Equifax, Inc. $150,000.[36] ;

- Other prevalent targets for identity theft are financial institutions (banks, credit card companies, securities companies, etc.), and government agencies (international, federal, state, and local); and

- The AARP analyzed 244 publicly disclosed security breaches from January 1, 2005 through May 26, 2006, identified by the Identity Theft Resource Center (ITRC).[37] An examination of the most frequent cause of reported security breaches reveals that a third (33%) of all breaches were caused by hackers who broke into computer systems to gain access to sensitive personal information. The analysis finds that educational institutions are more likely than any other type of entity to report having had a security breach. In fact, educational institutions were more than twice as likely to report suffering a breach as any other type of entity. Physical theft of computers, computer equipment, or paper files is the next most common cause of security breaches, followed by improper display.

---

[34] Dan Carnevale, "Why Can't Colleges Hold On to Their Data?," *Chronicle of Higher Education*, May 6, 2005, p. A35.

[35] Reuters, "U.S. Colleges Struggle to Combat Identity Theft," eWeek, Aug. 17, 2005, at [http://www.findarticles.com/p/articles/mi_zdewk/is_200508/ai_n14906864].

[36] Andrea L. Foster, "Louisiana State U. Signs Deal to Protect Students and Employees in Case of Data Breach," *Chronicle of Higher Education*, September 13, 2006, at [http://chronicle.com/daily/2006/09/2006091301t.htm].

[37] AARP, "Into the Breach: Security Breaches and Identity Theft," July 2006, at [http://www.aarp.org/research/frauds-scams/fraud/dd142_security_breach.html].

Table 1. Data Security Breaches in Businesses (2000-2006)

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Linden Labs (creator of Second Life virtual community)	September 2006	members of interactive virtual community	650,000	names, addresses, encrypted passwords, payment information	"Second Life' Suffers Real-world Breach," CNET.com, September 10, 2006, at [http://news.com.com/2100-7349_3-6114046.html]
Hospital Corporation of America (HCA) - stolen computers	August 2006	records from 1996 to 2006 for patients who had received treatment at hospitals managed by HCA in eight states (Colorado, Kansas, Louisiana, Mississippi, Oklahoma, Oregon, Texas and Washington)	unknown	billing records (details unknown)	Ferguson, Scott, "FBI Investigating Theft of 10 Hospital Computers," eWeek, August 21, 2006 at [http://www.eweek.com/print_article2/0,1217,a=186560,00.asp]
AT&T - hackers broke into computer system	August 2006	customers who purchased DSL equipment from AT&T online store	19,000	credit card data	*Associated Press*, "Hackers Gain Data on AT&T Shoppers," *New YorkTimes.com*, August 30, 2006.
Automated Data Processing (ADP) (Roseland, NJ) - "an unauthorized party impersonated officers" to obtain information on investors	July 2006	individual investors with 60 companies including Fidelity, UBS, Morgan Stanley , Bear Stearns, Citigroup, Merrill Lynch	hundreds of thousands	names, addresses, number of shares held of investors	Spangler, Todd, "ADP Duped into Disclosing Data,"BaselineMag.com, July 10, 2006, at [http://www.baselinemag.com/article2/0,1540,1986655,00.asp].

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Kaiser HMO - stolen laptop	July 2006	HMO subscribers to Kaiser health plan	160,000	names, phone numbers, Kaiser numbers	Singel, Ryan, "Kaiser Joins Lost Laptop Crowd," *InfoSecurity*, July 30, 2006, at [http://infosecurity.us/mambo//content/view/90/49/]
C.S. Stars (insurance contractor) - lost computer containing workers' records	July 2006	injured New York state workers (claiming compensation funds)	540,000	SSNs, names, addresses	Hines, Matt, "Insurance Company Loses 540,000 N.Y Employee Records," eWeek, July 26, 2006, at [http://www.eweek.com/article2/0,1895,1994416,00.asp]
National Association of Securities Dealers (NASD)-(Boca Raton, FL) - 10 stolen laptops	July 2006	securities dealers who were the subject of investigations involving possible misconduct.	73	SSNs of securities dealers, plus inactive account numbers of about 1,000 consumers	Jamieson, Dan, "Rule Likely on Notification of Data Breaches, Some Say; Theft of NASD Laptops Raises Questions about Regulators' security," *Investment News*, July 10, 2006, p. 2.
American Red Cross, Farmers Branch (Dallas, TX) - 3 stolen laptops	July 2006	regional blood donors	8,000	names, SSNs, birth dates, medical information	Schreier, Laura, "Donor Data Stolen at Local Red Cross Exclusive: 3 Laptops from Farmers Branch Office Held Encrypted Records," *Dallas Morning News*, July 1, 2006, p. 1A.
Bisys Group Inc.(Roseland, NJ) - employee's truck carrying backup tapes was stolen	July 2006	hedge fund donors	61,000	SSNs of 35,000 individuals	Clair, Chris, "Bisys Discloses Data Theft," *HedgeWorld Daily News*, July 6, 2006 (no page given).

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
American International Group (AIG)- burglary of a file server	June 2006	employees of various companies whose insurance information was submitted to AIG	970,000	names, addresses, SSNs, medical information	Smith, Elliot Blair, "AIG: Personal Data on 970,000 Lost in Burglary; Insurer Has Yet to Alert Those Affected by March 31 Break-in," *USA Today*, June 19, 2006, p. 5B.
Ernst & Young- stolen laptop	June 2006	Hotels.com customers	243,000	names, credit card numbers	Reilly, David, "Hotels.com Credit-Card Data Lost in Stolen Laptop Computer," *Wall Street Journal*, June 2, 2006, p. A14.
Union Pacific- stolen laptop	June 2006	employees of the railroad company	30,000	personal data	Vijayan, Jaikumar and Todd Weiss, "Flurry of New Data Breaches Disclosed," Computerworld, June 19, 2006 at [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001282].
Ross-Simmons- data breach	April 2006	customers	undisclosed	credit card numbers, financial information, other personal information	"Ross-Simons Says Security Breach Exposes Customers," Computerworld, April 12, 2006, at [http://www.computerworld.com/securitytopics/security/story/0,10801,110425,00.html?source=x3888].

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
EBay- hackers harvesting and selling user information	March 2006	customers	undisclosed	account information	Niccolai, James, "Russian Web Site Offered eBay Account Info for $5," Computerworld, March 24, 2006, at [http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,109881,00.html].
Deloitte & Touche- unencrypted CD left on a plane	February 2006	all U.S. and Canadian employees of McAfee Software hired before April 2005	9,200	names, SSNs, McAfee stock holdings	Kuruvila, Matthai C., "Security Giant's Data Lost," *Silicon Valley*, February 24, 2006.
Atlantis Resort- theft from the hotel's database	January 2006	customers	55,000	names, addresses, credit card details, SSNs, driver's license numbers, bank account data	"IDs of 50,000 Bahamas Resort Guests Stolen," CNet News, January 10, 2006.
Guidance Software- hacker	December 2005	security researchers and law enforcement agencies worldwide	3,800	credit card numbers	Krebs, Brian, "Hackers Break Into Computer-Security Firm's Customer Database," *Washington Post* December 19, 2005, p. D5.
Sam's Club- "card-skimming" devices	December 2005	customers who bought fuel at its gas stations between September 21 and October 2.	600	credit card information	Vijayan, Jaikumar, "Card Skimmers Eyed in Sam's Club Data Theft," Computerworld, December 14, 2005, at [http://www.computerworld.com/databasetopics/data/story/0,10801,107067,00.html].

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Marriott Vacation Club International- missing data tapes	December 2005	customers and employees	206,000	addresses and credit card information	"Marriott Vacation Club reports missing data tapes," Computerworld, December 26, 2005, at [http://computerworld.com/securitytopics/security/story/0,10801,107366,00.html?SKC=security-107366].
Ford Motor Company- stolen computer	December 2005	current and former Ford employees	70,000	names and SSNs	"Tech Crime Gets Personal at Ford," CNN Money, December 22, 2005, at [http://money.cnn.com/2005/12/22/news/fortune500/ford_theft/].
Safeway - company laptop stolen from manager's home	November 2005	employees	1,200	names, SSNs, hire dates and work locations	Akkad, Dania, "Safeway Discloses Security Breach,"*Monterey County Herald*, November 5, 2005 (no page given).
Boeing - theft of company computer	November 2005	current and former Boeing workers	161,000	names, Social Security numbers (SSNs), some birth dates and banking information for employees who elected to use direct deposit of payroll	Bowermaster, David and Dominic Gates and Melissa Allison, "161,000 Workers' Personal Data on PC Stolen from Boeing," *Seattle Times*, November 19, 2005, p. A1.
Eastman Kodak - laptop stolen from a consultant's locked car trunk.	June 2005	former Eastman Kodak workers	5,800	names, Social Security numbers, birth dates and benefits information	Davia, Joy, "Kodak Warns of Data Theft," *Rochester Democrat and Chronicle (New York)*, June 22, 2005, p. 8D.

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Time Warner - loss of 40 computer backup tapes containing sensitive data while being shipped by Iron Mountain to an offsite storage center	May 2005	current and former employees, some of their dependents and beneficiaries, and individuals who provided services for the company	600,000	names, SSNs	Zeller, Tom, "Time Warner Says Data on Employees Is Lost," *New York Times*, May 3, 2005, p. C4.
MCI - laptop stolen from a car that was parked in the garage at the home of a MCI financial analyst	May 2005	current and former employees	16,500	names and SSNs	Young, Shawn, "MCI Reports Loss Of Employee Data On Stolen Laptop," *Wall Street Journal*, May 23, 2005, p. A2.
LEXIS/NEXIS - intruders used passwords of legitimate customers to get access to a Seisint database called Accurint, which sells reports to law-enforcement agencies and businesses. Later analysis determined that its databases had been fraudulently breached 59 times using stolen passwords.	March 2005	customers	32,000 (subsequent investigation reveals the actual number is 310,000)	names, addresses, passwords, SSNs, drivers license	El-Rashidi, Yasmine, "LexisNexis Reports Data Breach; Personal Records Are Hacked as Concerns About Security and Identity Theft Intensify," *Wall Street Journal*, March 10, 2005, p. A3; and Krim, Jonathan, "LexisNexis Data Breach Bigger Than Estimated: 310,000 Consumers May Be Affected, Firm Says," *Washington Post*, April 13, 2005, p. E1.

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
DSW Shoe Warehouse store - information stolen from computer database over 3- month period	March 2005	customers of 103 of the chain's 175 stores	initially "hundreds of thousands," then raised to 1.4 million	credit card information	*Associated Press*, "DSW ID Theft May Affect Over 100,000," *Chicago Tribune*, March 11, 2005, p. 4; and "Firm Raises Data Theft Count," *Washington Post*, April 19, 2005, p. E2.
T-Mobile - hacker intrusion into company database	February 2005	T-Mobile customers	400	customer records, passwords, SSNs, private e-mail and candid celebrity photos **note**: data offered for sale via online forum	Poulsen, Kevin, "Known Hole Aided T-Mobile Breach,"Wired News, February 28, 2005, at [http://www.wired.com/news/privacy/0,1848,66735,00.html].
Motorola - Thieves broke into the offices of Affiliated Computer Services (ACS), a provider of human resources services, and stole two computers	June 2005	Motorola employees	34,000 in U.S.	SSNs and personal information	"Two Computers Stolen with Motorola Staff Data," Reuters, June 10, 2005.
ChoicePoint - criminals used fake documentation to open 50 fraudulent accounts to access consumer data	February 2005	consumers	30,000-35,000 in California; 145,000 nationwide	names, addresses, SSNs, credit reports	Perez, Evan, "ChoicePoint Is Pressed to Explain Database Breach," *Wall Street Journal*, February 5, 2005, p. A6.

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Affiliated Computer Services - inmate hacked into county database	October 2004	county employees	900	names, birth dates, SSNs, bank account routing numbers and checking account numbers	Whaley, Monte, "FBI on Weld ID-Theft Case Feds to Analyze Data from Cell of Inmate Who Hacked Computer," *Denver Post*, November 11, 2004, p. B1.
Lowe's (home improvement store) - hacker used vulnerable wireless network to attempt to steal credit card info	June 2004	customers	unknown	skimmed credit account information for every transaction processed at a particular Lowe's store	Roberts, Paul, "Wireless Hacker Pleads Guilty: Man Admits Using Store's Wireless Network to Steal Credit Card Info," PC World, June 7, 2004, at [http://msn.pcworld.com/news/article/0,aid,116411,00.asp].
eBay - hackers tricked online merchants who used the PayPal payment processing system into disclosing their user names and passwords, then logged onto the merchants' accounts	March 2004	several eBay merchants	company did not disclose	customer names, e-mail addresses, home addresses and transactions	Kirby, Carrie, "New Scam Threat at eBay / Hackers Obtained Information on Some Customers," *San Francisco Chronicle*, March 16, 2004, p. C1.
Kinko's - hacker installed a key logger to record every character typed on 13 Kinko's computers	November 2003	Customers at Internet terminals at 13 Kinko's copy shops in Manhattan	450	SSNs, names, passwords, credit cards, bank account data **note:** data was sold	Napoli, Lisa, "A Hacker Masters Keystroke Theft: Personal Data Stolen from 450 Victims," *International Herald Tribune*, August 9, 2003, p. 1.

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Acxiom (marketing company) - hacker downloaded data	August 2003	clients include 14 of the top 15 credit card companies, 5 of the top 6 retail banks, IBM, Microsoft, and federal government	10% of clientele (no total number given)	passwords, personal, financial, and company information	Lee, W.A. "Hacker Breaches Acxiom Data," *American Banker*, August 11, 2003, p. 5.
DirecTV - hacker stole trade secrets for access card	April 2003	DirecTV subscribers	50,000 customers used counterfeit access cards to watch programming without paying	details about the design and architecture of DirecTV's "Period 4" cards **note**: data was sold	"U. of C. Student Pleads Guilty to Theft of Direc TV Card Data ; Trade Secrets Ended up on Hacker Site, Enabling Free Access," *Chicago Sun-Times*, April 30, 2003, p. 16.
TCI help-desk worker sold client access codes to two others, who then used the codes to obtain more than 15,000 customer credit records	November 2002	credit reporting bureau customers	15,000 (Wired News) 30,000 (*Seattle Times*)	names, addresses, SSNs, credit card **note:** data sold, for $60 per record	Delio, Michelle, "Cops Bust Massive ID Theft Ring," Wired News, November 25, 2002, at [http://www.wired.com/news/privacy/0,1848,56567,00.html]; and Masters, Brooke, "Huge ID-Theft Ring Broken; 30,000 Consumers at Risk ; Men Charged with Stealing Personal, Financial Data ," *Seattle Times*, November 26, 2002, p. A1.

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Midwest Express Airlines and Federal Aviation Administration - hackers posted list of customer names to website and posted a list of airport security screening results taken from the FAA's system	April 2002	Midwest Express Airlines customers; FAA (two separate incidents)	unknown	passenger names and airport security screening results	Larson, Virgil, "Computer Hackers Breach Midwest Express Systems," *Omaha World-Herald*, April 22, 2002, p. 1D.
ChoicePoint - Nigerian-born brother and sister posed as legitimate businesses to set up ChoicePoint accounts	2002	unknown	7,000-10,000 inquiries on names and SSNs, then used identities to commit fraud	names and SSNs **note:** data was sold	*Associated Press*, "ChoicePoint Suffered Previous Breach: Two ID Thieves Arrested in 2002 for Tapping into Data" MSNBC, February 3, 2005, at [http://www.msnbc.msn.com/id/7065902/].
New York City restaurant busboy duped credit reporting companies into providing detailed credit reports	March 2001	chief executives, celebrities and tycoons from Forbes list of richest Americans	200	SSNs, home addresses and birth dates, credit card numbers	Hays, Tom, "Busboy Hacks Only the Richest, Used Forbes' List in Plot to Steal Identity, Credit Info, Big Bucks," *Pittsburgh Post-Gazette*, March 21, 2001, p. A11.

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
World Economic Forum - hackers broke into computer	February 2001	attendees	3,200	passport numbers, cell phone numbers, credit card numbers, exact arrival and departure times, hotel names, room numbers, number of overnights, sessions attended, plus information on 27,000 people who have attended the global forum in recent years	Higgins, Alexander, "Hackers Steal World Leaders' Personal Data," *Chicago Sun-Times*, February 6, 2001, p. 20.
International credit card ring adds fraudulent charges of 277 Russian rubles ($5-10) to credit cards	January 2001	Internet shopping sites	unknown	credit card numbers **note:** data was sold	James, Michael, "Small-time Thefts Reap Big Net Gain Tens of Thousands of Phony $5-$10 Credit-Card Charges Rake in Millions for Hackers," *Orlando Sentinel*, January 27, 2001, p. E5.
Egghead - hacker attacked computer system	December 2000	customers	3.5 million credit card accounts; 7500 of which showed "suspected fraudulent activity"	credit card info	"Sayer, Peter, "Egghead Says Customer Data Safe After Hack Attack," PC World, January 8, 2001 at [http://msn.pcworld.com/news/article/0,aid,37781,00.asp].

Business Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Western Union - hackers made electronic copies of the credit and debit card information	September 2000	customers who transferred money on a company website	15,700	credit and debit card information	Cobb, Alan, "Hackers Steal Credit Card Info from Western Union Site," *Chicago Sun-Times*, September 11, 2000, p. 22.
America Online - AOL customer-service representatives mistakenly downloaded an e-mail attachment sent by hackers	June 2000	customers	500 records were viewed	names, addresses, and credit card numbers	"Hackers Breach Security At America Online Inc," *Wall Street Journal*, June 19, 2000, p. A34.
Two British teens intruded into 9 e-commerce websites in the United States, Canada, Thailand, Japan and Britain	March 2000	customers	26,000 credit card accounts	credit card data **note:** some data was posted on the Web	Sniffen, Michael, "2 Teens Accused of Hacking Charged in $3 Million Credit Card Theft," *Chicago Sun-Times*, March 25, 2000, p. 9.
CD Universe (online music store) - hacker stole credit card numbers and released thousands of them on a website when the company refused to pay a $100,000 ransom	January 2000	customers	300,000	credit card numbers **note**: Maxus Credit Card Pipeline Website posted up to 25,000 stolen numbers	*Associated Press*, "Hacker Said to Steal 300,000 Card Numbers," *Arizona Republic*, January 11, 2000, p. A3.
Pacific Bell - 16-year-old teenager hacked into server and stole passwords	January 2000	subscribers	63,000 accounts were decrypted; 330,000 customers told to change passwords	passwords	Gettleman, Jeffrey, "Passwords of PacBell Net Accounts Stolen; Computers: Authorities Say 16-year-old Hacker Took the Data for Fun. Theft Affects 63,000 Customers," *Los Angeles Times*, January 12, 2000, p. 2.

Table 2. Data Security Breaches in Education (2000-2006)

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Western Illinois University-hacker accessed several electronic student services systems	July 2006	students, customers of the university's online bookstore, guests of the university hotel	180,000	SSNs, personal data, credit card information	Maguire, John, "Alums Just Told of Computer Breach: Data on 180,000 with Ties to WIU Hacked a Month Ago," *Chicago Sun-Times*, July 5, 2006, p. 8.
University of Tennessee - hacker broke into UT computer	July 2006	past and current employees	36,000	SSNs, names, addresses	Herrington, Angie, "UT Notifies Workers of Computer Hacking,"*Chattanooga Times Free Press*, July 7, 2006, p. O.
Northwestern University (Chicago) - hackers broke into nine desktop computers in the Office of Admissions and Financial Aid	July 2006	students and applicants to the school	17,000	names, addresses, SSNs	"Hackers break into NU Admissions, Financial Aid Computers," *Chicago Sun Time*s, July 15, 2006, at [http://www.suntimes.com/cgi-bin/print.cgi?getReferrer=[http://www.suntimes.com/output/news/cst-nws-hack15.html].
Moraine Park Technical College (Beaver Dam, Fond du Lac, & West Bend, WI) - missing computer disk	July 2006	apprenticeship students back to 1993	1,500	names, addresses, phone numbers, SSNs	"News Summaries Ozaukee and Washington Counties," *Milwaukee Journal Sentinel*, July 16, 2006, p. Z3

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Catawba County Schools (Newton, NC) - website exposed personal data	June 2006	students who had taken keyboarding and computer applications placement test during the 2001-02 school year	619	names, SSNs, test scores	Shain, Andrew, and Hannah Mitchell, "619 Students' Secure Data Revealed Online: Google Page Showed Social Security Numbers, Test Scores, *Charlotte Observer*, June 24, 2006, p. 1B.
San Francisco State University - faculty member's laptop stolen	June 2006	current and former students	3,000	names, SSNs, phone numbers and grade point averages.	Asimov, Nanette, "SFSU students' information stolen; School alerts 3,000 affected by theft of faculty laptop," *San Francisco Chronicle*, June 23, 2006, p. B5.
University of Kentucky- stolen thumb drive	June 2006	current and former students	6,500	SSNs	Kiernan, Vincent, "Incidents at Two Universities Put More Than 200,000 Students at Risk of Data Theft," *The Chronicle of Higher Education*, June 19, 2006, p. A21

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Ohio University (Athens, OH) - hackers breach servers in two separate incidents	May 2006	individuals and organizations listed in the alumni database, owners of patents and other intellectual property	300,00	SSNs, personal information, biographical information, patent data, intellectual property files	Vijayan, Jaikumar, "Ohio University Reports Two Separate Security Breaches," Computerworld, May 3, 2006, at [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=111113&intsrc=article_pots_bot].
Sacred Heart University- hackers intrude system	May 2006	students and some individuals not associated with the university	135,000	personal information, SSNs	Sandoval, Greg, "Sacred Heart is Latest University to be Hacked," CNet News, May 26, 2006, at [http://news.com.com/2100-7349_3-6077212.html].
University of Texas, Austin- data breach	April 2006	students, alumni, faculty, and staff of the business school	200,000	SSNs, biographical materials	*Associated Press*, "University of Texas Probes Computer Breach," MSNBC, April 24, 2006, at [http://www.msnbc.msn.com/id/12459840/].
University of Arizona- hackers break into journalism department's computer system	February 2006	journalism students	undisclosed	none so far	Grossman, Djamila, "Romanian Hacker Breaks into UA Journalism Computers," *Arizona Daily Star*, February 14, 2006, p. B2.

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Notre Dame- hackers attack server	January 2006	alumni and other donors to the university	undisclosed	SSNs, credit card numbers, check images	Roberts, Paul F., "Hackers Target Notre Dame Donors," eWeek, January 24, 2006, at [http://www.eweek.com/article2/0,1895,1915087,00.asp].
Indiana University - malicious software programs installed on business instructor's computer	November 2005	Kelly School of Business students enrolled in introductory business course between 2001-2005	5,300	personal student information	*Associated Press*,"IU Finds 'Malicious' Software," FortWayne.com, November 18, 2005, at [http://www.fortwayne.com/mld/fortwayne/news/local/13202338.htm].
University of Tennessee Medical Center - laptop computer stolen	November 2005	patients who received treatment in 2003	3,800	names and SSNs	"UT Patients Warned of Stolen Computer," *Chattanooga Times Free-Press*, November 2, 2005, p. B2.
Georgia Institute of Technology Office of Enrollment Services - computer theft	November 2005	past, present, and prospective students	13,000	SSNs, birth dates, names, addresses	Kantor, Arcadiy, "Georgia Tech Computer Theft Compromises Student Data," *The Technique* (via University Wire), November 11, 2005 at [http://www.nique.net/issues/2005-11-11/news/3].

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
University of Tennessee - inadvertent posting of names and Social Security numbers to Internet lists	October 2005	students and employees	1,900	names and SSNs	"State Briefs: UT Students' Private Data Posted on the 'Net," *The* Tennessean.com, October 29, 2005, at [http://tennessean.com/apps/pbcs.dll/article?AID=/20051029/NEWS01/510290327/1006/NEWS01].
University of Georgia - hacker hits employee records server	September 2005	current and former employees of university's College of Agricultural and Environmental Sciences	1,600	SSNs	Simmons, Kelly, "Hackers Breach Database at UGA," *The Atlanta Journal - Constitution*, September 29, 2005, p. C2.
Miami University (Ohio) - report containing SSNs and grades of more than 20,000 students has been accessible via the Internet since 2002	September 2005	students	21,762	SSNs, grades	Giordano, Joe, "Miami University, Ohio, Finds Huge Online Security Breach," *Journal-News (Hamilton, OH)*, September 16, 2005 (no page given).
Kent State University - five desktop computers stolen from campus	September 2005	students and professors	100,000	names, SSNs, grades	Gonzalez, Jennifer, "Student, Faculty Data on Stolen Computers," *Plain Dealer (Cleveland)*, September 10, 2005, p. B1.

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Sonoma State University - hacking	August 2005	people who either attended, applied, graduated or worked at the school from 1995 to 2002	61,709	names, SSNs	Park, Rohnert, "Hackers Hit College Computer System: Identity Theft Fears at Sonoma State," *San Francisco Chronicle*, August 9, 2005, p. B2.
California State University - Office of the Chancellor may have experienced unauthorized access to one of its computers	August 2005	students who receive financial aid and two financial aid administrators	154	names, SSNs	"California State University Chancellor's Office Experiences Potential Computer Security Breach,"*U.S. States News*, August 29, 2005 (no page given).
University of Florida Health Sciences Center/ChartOne - stolen laptop	August 2005	patients and physicians	3,851	names, SSNs, dates of birth, medical records	Chun, Diane, "3,851 Patients at Risk of ID Theft," *Gainesville.com*, August 27, 2005 at [http://www.gainesville.com/apps/pbcs.dll/article?AID=/20050827/LOCAL/208270336/1078/news].
University of Colorado - hacking into campus Card Office (creates IDs for staff and students)	August 2005	students and faculty	36,000	university accounts and personal information	Uhls, Anna, "U. Colorado students getting (re)carded," *University Wire/Colorado Daily*, August 4, 2005 (no page given).

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
University of North Texas - hacking	August 2005	current, former and prospective students	38,607	names, addresses, telephone numbers, SSNs, student identification numbers, student ID passwords, student classification information and possibly 524 credit card numbers	Tessyman, Neal, "Hackers Steal Student Info from U. North Texas," *University Wire*, August 11, 2005 (no page given).
University of Colorado - hackers tapped into a database in the registrar's office	August 2005	student records from June 1999 to May 2001 and from fall 2003 to summer 2005.	49,000	names, SSNs, addresses, phone numbers	Mccrimmon, Katie Kerwin, "Hackers Tap CU Registrar's Database; Privacy of 49,000 Students Potentially Invaded in Breach," *Rocky Mountain News* (Denver), August 20, 2005, p. 20A.
California State University, Stanislaus - hacking	August 2005	student workers	900	names, SSNs	Togneri, Chris, "Hacker Breaks into Stan State Computer," *Modesto Bee*, August 16, 2005, p. B1.
University of Southern California - individual hacked into USC's online application system	July 2005	applicants	270,000	name, address, SSNs, e-mail address, phone number, date of birth, login information	Hawkins, Stephanie, "Hacker Hits Application System at USC," *University Wire/ Daily Trojan*, August 18, 2005 (no page given).

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
California Polytechnic, Pomona - two computers hacked	July 2005	university applicants and current and former faculty, staff and students	31,077	names, SSNs	Ruiz, Kenneth, "Hackers Infiltrate Cal Poly," *Whittier Daily News (CA)*, August 5, 2005 (no page given).
University of Colorado, Boulder - hackers broke into a computer server containing information used to issue identification cards	July 2005	students and professors	29,000 students and 7,000 professors	SSNs, names, photographs	*Associated Press*, "Hackers Break into CU Computers Containing 36k Records," August 1, 2005.
Michigan State University - breach of a server in the College of Education	July 2005	students	27,000	names, addresses, SSNs, course information, personal identification numbers	*Associated Press*, "Students Informed Social Security Numbers Possibly Compromised," July 7, 2005.
University of California, San Diego - hackers broke into university server	July 2005	students, staff, faculty who had attended or worked at UCSD Extension in the past five years	3,300	SSNs, driver license and credit card numbers	"SD UCSD Hackers," *City News Service*, July 1, 2005 (no page given).
California State University Dominguez Hills - hacking	July 2005	students	9613	names, SSNs	*Associated Press*, "Hackers crack computers, access private student information," July 29, 2005.

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
University of Connecticut - hacking - rootkit (collection of programs that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network) placed on server on October 26, 2003, but not detected until July 20, 2005	June 2005	students, staff, and faculty	72,000	names, SSNs, dates of birth, phone numbers and addresses	Naraine, Ryan, "UConn Finds Rootkit in Hacked Server," eWeek, June 27, 2005, at [http://www.eweek.com/article2/0,1759,1831892,00.asp].
Kent State University - laptop stolen from employee's car	June 2005	full-time faculty members since 2001	1,400	names, SSNs	Hampp, David, "Kent State U. Faculty Affected by Stolen Computer," *Daily Kent Stater* (via University Wire), June 22, 2005 (no page given).
Ohio State University Medical Center - two stolen laptops	June 2005	patients	15,000	patient names, admission and discharge dates, whether the patient had insurance, total charges and adjustments to the account.	Crane, Misti, "Laptop Containing Patients' Billing Information Stolen; Birth Dates, Social Security Numbers Not in Data Taken from Consultant, Osu Says," *Columbus Dispatch (OH)*, June 30, 2005, p. 4C.

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
University of Hawaii - dishonest library worker indicted on federal charges of bank fraud related to identity theft	June 2005	students, faculty, staff and library patrons at any of the 10 campuses between 1999 and 2003	150,000	SSNs, addresses and phone numbers	*Associated Press*, "UH Warns of Possible Identity Theft," June 19, 2005.
Jackson Community College (MI)- hacker breaks into computer system	May 2005	employees and students of the college	8,000	SSNs	"Computer Crime: Hacker May Have Stolen Social Security Numbers From Jackson Community Collegea," *Computer Crime Research Center*," May 29, 2005 (no page given).

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Carnegie Mellon University - security breach of school's computer network	May 2005	graduates of the Tepper School of Business from 1997 to 2004; current graduate students; applicants to the doctoral program from 2003 to 2005; applicants to the MBA program from 2002 to 2004; and administrative employees	5,000	SSNs and personal information	*Associated Press*, "Carnegie Mellon Reports Computer Breach," MSNBC, April 21, 2005, at [http://msnbc.msn.com/id/7590506/]
Stanford University- computer system breach	May 2005	students and recruiters of the university	9,600	SSNs, resumes, financial data, government information	Musil, Steven, "FBI Probes Network Breach at Stanford," CNet News, May 25, 2005.
Florida International University (FIU) - a hacker acquired user names and passwords for 165 computers on campus	May 2005	faculty and students	unknown	SSNs, credit card numbers	Leyden, John, "Florida Univ on Brown Alert after Hack Attack," *The Register*, April 29, 2005, at [http://www.theregister.com/2005/04/29/fiu_id_fraud_alert/].

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Northwestern University (Kellog School of Management) - computer network breach	May 2005	faculty, students, and alumni	17,500	user IDs and passwords	Meglio, Francesca Di, "Hacker Break-In," *Computer Crime Research Center*, May 23, 2005 (no page given).
University of California, San Francisco - hacker gained access to server used by accounting and personnel department	April 2005	students, faculty and staff	7,000	names and SSNs numbers	Lazarus, David, "Another Incident for UC," *San Francisco Chronicle*, April 6, 2005, p. C1.
Tufts University - possible security breach in an alumni and donor database after abnormal activity on the server in October and December, 2004	April 2005	alumni	106,000	SSNs and other unspecified personal information	Roberts, Paul, "Tufts Warns 106,000 Alumni, Donors of Security Breach: Personal Data on a Server Used for Fund Raising May Have Been Exposed," Computerworld, April 13, 2005, at [http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,101043,00.html?source=x10].
University of Nevada, Las Vegas - hackers accessed school's Student and Exchange Visitor Information System (SEVIS) database	March 2005	current and former students and faculty	5,000	personal records, including birth dates, countries of origin, passport numbers, and SSNs	Lipka, Sara, "Hacker Breaks Into Database for Tracking International Students at UNLV," *Chronicle of Higher Education*, March 21, 2005, p. A43.

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
California State University, Chico - hackers broke into servers	March 2005	students, former students, prospective students, and faculty	59,000	SSNs	*Associated Press*, "Hackers Gain Personal Information of 59,000 People Affiliated with California University,"*Grand Rapids Press*, March 22, 2005, p. A2.
University of California, Berkeley laptop stolen from restricted area of campus office	March 2005	alumni, graduate students, and past applicants	100,000	SSNs numbers, names; addresses, and birth dates for 1/3 of affected people	Liedtke, Michael, "Laptop Theft Causes Identity Fraud Worry," *Daily Breeze* (Torrance, CA), March 28, 2005, p. A10.
George Mason University - hackers gained access to information	January 2005	faculty, staff, and students	30,000	names, photos, SSNs, and campus ID numbers	McCullagh, Declan, "Hackers Steal ID Info from Virginia University," Wired News, January 10, 2005, at [http://news.com.com/2100-7349_3-5519592.html].
University of California, San Diego (UCSD) - hacker breached computer system	January 2005	students and alumni of UCSD Extension	3,500	names, SSNs	Yang, Eleanor, "Hacker Breaches Computers That Store UCSD Extension Student, Alumni Data," *San Diego Union Tribune*, January 18, 2005, p. B3.

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
University of California, Berkeley - hacker compromised the university's computer system	October 2004	Californians participating in California's In-Home Supportive Services program since 2001	1.4 million individuals	SSNs, names, addresses, phone numbers, and dates of birth	Reuters, "Hacker Strikes University Computer System,"CNET News, October 19, 2004, at [http://news.com.com/2100-7349_3-5418388.html].
California State - auditor from chancellor's office lost hard drive containing personal information	August 2004	380,000 current and former students, applicants, staff, faculty and alumni at UC San Diego and 178,000 at San Diego State	23,500	name, address, SSNs	Connell, Sally Ann, "Security Lapses, Lost Equipment Expose Students to Possible ID Theft; in the Latest Incident, a Cal State Hard Drive with Data on 23,500 Individuals Is Missing," *Los Angeles Times*, August 29, 2004, p. B4.
University of California, Los Angeles - stolen laptop w/ blood donor info	June 2004	blood donors	145,000	names, birth dates and SSNs	Becker, David, "UCLA Laptop Theft Exposes ID Info,"CNET News, October 6, 2004, at [http://news.com.com/UCLA+laptop+theft+exposes+ID+info/2100-1029_3-5230662.html?tag=nl].

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
University of California, San Diego (UCSD) - hackers breached security at the San Diego Supercomputer Center and the University's Business and Financial Services Department	April 2004	UCSD students, alumni, faculty, employees and applicants	380,000	SSNs, and driver license numbers	Sidener, Jonathan, "SD Supercomputer Center Among Victims of Intrusion," *San Diego Union Tribune*, April 15, 2004, p. B3.
Georgia Institute of Technology	March 2003	patrons of art and theatre program	57,000	credit card numbers	Lemos, Robert, "Data Thieves Strike Georgia Tech," Wired News, March 31, 2003, at [http://news.com.com/Data+thieves+strike+Georgia+Tech/2100-1002_3-994821.html?tag=nl].
University of Texas, Austin - computer hackers broke into database on multiple occasions	March 2003	current and former student, faculty and staff members, as well as job applicants	55,200	names, addresses, SSNs, email addresses, office phone numbers **note:** perpetrator claimed he did not distribute the numbers and had not used them "to anyone's detriment"	Read, Brock, "Hackers Steal Data From U. of Texas Database," *Chronicle of Higher Education*, March 21, 2003, p. 35.
University of Kansas - hacker break-in to Student and Exchange Visitor Information System (SEVIS)	January 2003	foreign students	1,400	SSNs, passport numbers, countries of origin, and birth dates.	Arnone, Michael, "Hacker Steals Personal Data on Foreign Students at U. of Kansas,"*Chronicle of Higher Education*, January 24, 2003 (no page given).

Education Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
College of the Canyons (California) - computer hard drive containing personal student information stolen	October 2001	current and former students	36,000	names, SSNs, and photographs	Mistry, Bhavna, "Identity Theft Alert Issued at College," *Los Angeles Daily News*, October 21, 2001, p. N7.
University of Washington Medical Center - hacker broke into computer system	December 2000	cardiology and rehabilitation patients	5,000	names, addresses, birth dates, heights and weights, SSNs, and the medical procedure undergone	"Hacker Steals Patient Records," *San Diego Union-Tribune*, December 9, 2000, p. A3.

Table 3. Data Security Breaches in Financial Institutions (2001-2006)

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
ING Financial Services- stolen laptop	June 2006	District of Columbia government workers and retirees	13,000	SSNs, personal data	Dwyer, Timothy, "ING Financial to Notify Potential Identity Theft Victims," *Washington Post*, June 19, 2006, p. B4.
Equifax Inc.- stolen laptop	June 2006	nearly all the U.S. employees of the credit reporting bureau	2,500	names, SSNs	Stempel, Jonathan, "Equifax Says Laptop With Employee Data Was Stolen," eWeek, June 20, 2006, at [http://www.eweek.com/article2/0,1759,1979296,00.asp?kc=EWRSS03129TX1K0000614].
Fidelity Investments- stolen laptop	March 2006	Hewlett-Packard employees	196,000	personal data	Hines, Matt, "Stolen Fidelity Laptop Exposes HP Workers," eWeek, March 23, 2006, at [http://www.eweek.com/article2/0,1895,1942049,00.asp].
Bank of America, Washington Mutual- debit cards cancelled	February 2006	customers using debit cards issued by the two banks at Sam's Club gas stations and Office Max	200,000	debit card information which was used to accrue fraudulent charges	Sandoval, Greg "Web of Intrigue Widens in Debit-Card Theft Case," CNet News, February 13, 2006, at [http://news.com.com/Web+of+intrigue+widens+in+debit-card+theft+case/2100-1029_3-6038405.html].

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Ameriprise Financial- laptop theft	January 2006	customers and advisers with the financial firm	230,000	names, SSNs, internal account numbers	Dash, Eric, "Ameriprise Loses Data on 230,000 Customers and Advisers," *New York Times*, January 25, 2006.
H&R Block- Social Security numbers printed on unsolicited packages containing free software	January 2006	recipients of the company's tax preparation software	undisclosed	SSNs	Gilbert, Alorie, "H&R Block Blunder Exposes Consumer Data," CNet News, January 3, 2006, at [http://news.com.com/H38R+Block+blunder+exposes+consumer+data/2100-1029_3-6016720.html].
Visa USA	December 2005	customers with Visa cards from various financial institutions using a mutual merchant	undisclosed	credit card information	Weinstein, Natalie, "Visa Deals With Possible Data Breach," CNet News, December 24, 2005, at [http://news.com.com/2100-1029_3-6007759.html].
Scottrade Inc.- internet hacker	December 2005	customers of the stock brokerage firm	140,000	names, birth dates, drivers license numbers, phone numbers, bank names, bank routing numbers, bank account numbers, and Scottrade account numbers	"Hackers Reveal 140,000 Customer ID's," *Computer Crime Research Center*, December 2, 2005 (no page given).
TransUnion (credit reporting bureau) - stolen desktop computer	November 2005	customers	3,600	SSNs and personal credit information	Paul, Peralte, "Credit Bureau Burglary Leaves 3,600 Vulnerable," *Atlanta Journal and Constitution*, November 11, 2005, p. 5G.

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Choicepoint - Miami-Dade County Police Department may have misused the department's account to illegally access consumer records	September 2005	consumers	5,103	SSNs, driver's license information	Husted, Bill, "Another Breach of Records Feared; Choicepoint Tells 5,103 Customers about Incident," *Atlanta Journal-Constitution*, September 17, 2005, p. 1H.
Bank of America - stolen laptop	September 2005	Visa Buxx card users	undisclosed	names, credit card numbers, bank account numbers, routing transit numbers	McMillan, Robert, "Bank of America Notifying Customers After Laptop Theft," Computerworld, October 7, 2005, at [http://www.computerworld.com/securitytopics/security/story/0,10801,105246,00.html].
J.P. Morgan (Dallas) - stolen laptop	August 2005	clients	unknown	personal and financial information	"Security Breach at J.P. Morgan Private Bank,"*AFX International Focus*, August 30, 2005 (no page given).
Citigroup - a box of computer tapes with account information for 3.9 million customers was lost in shipment by CitiFinancial, a unit of Citigroup	June 2005	personal and home equity loan customers	3.9 million	names, addresses, SSNs and loan-account data	Krim, Jonathan, "Customer Data Lost, Citigroup Unit Says:3.9 Million Affected As Firms' Security Lapses Add Up, *Washington Post*, June 7, 2005, p. A1.

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Japanese credit cardholders - hackers behind U.S. data theft may have compromised the data of Japanese cardholders, according to the government. Fraudulent transactions have now emerged in Japan.	June 2005	customers of 26 domestic Japanese credit card firms	unknown	unknown	"Japan Cardholders 'Hit' by Theft,"*BBC News*, June 21, 2005 at [http://news.bbc.co.uk/2/hi/business/4114252.stm].
MasterCard - breach occurred in 2004 at a processing center in Tucson operated by CardSystems Solutions, one of several companies that handle transfers of payment between the bank of a credit card-using consumer and the bank of the merchant where a purchase was made. CardSystems' computers were breached by malicious code that allowed access to customer data.	June 2005	MasterCard credit card and some debit card customers	40 million	names, account numbers, security codes, expiration dates	Krim, Jonathan and Michael Barbaro, "40 Million Credit Card Numbers Hacked: Data Breached at Processing Center,"*Washington Post*, June 18, 2005, p. A1; Zeller, Tom and Eric Dash, "MasterCard Says 40 Million Files Put at Risk,"*New York Times*, June 18, 2005, p. A1; and Evers, Joris, "Credit Card Suit Now Seeks Damages," CNET News.com, July 7, 2005, at [http://news.com.com/Credit+card+suit+now+seeks+damages/2100-7350_3-5777818.html].
Bank of America - laptop stolen from car in Walnut Creek, CA	June 2005	California customers	18,000	names, addresses, SSNs,	Lazarus, David, "Breaches in Security Require New Laws," *San Francisco Chronicle*, June 29, 2005, p. C1.

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
New Jersey cybercrime ring stole financial records from bank accounts	May 2005	customers of four banks (Charlotte, North Carolina-based Bank of America and Wachovia, Cherry Hill, New Jersey-based Commerce Bank, and PNC Bank of Pittsburgh)	700,000	names, SSNs, bank account information **note:** bank employees sold financial records to collection agencies and law firms.	Weiss, Todd, "Scope of Bank Data Theft Grows to 676,000 Customers: Bank Employees Used Computer Screen Captures to Snag Customer Data," Computerworld, May 20, 2005, at [http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101903,00.html].
Ameritrade (securities broker) - loses tapes with back-up information on customer accounts	April 2005	Ameritrade current and former customers	200,000	account information	"Ameritrade Loses Customer Account Info," CNN Money, April 19, 2005, at [http://money.cnn.com/2005/04/19/technology/ameritrade/index.htm].
HSBC (global bank) sent out warning letters notifying customers that criminals may have gained access to credit card info	April 2005	holders of General Motors MasterCard who had shopped at Polo Ralph Lauren stores	180,000	credit card information	"Security Scare Hits HSBC's Cards,"*BBC News*, April 14, 2005, at [http://news.bbc.co.uk/2/hi/business/4444477.stm]; and Vijayan, Jaikumar, "Update: Scope of Credit Card Security Breach Expands," Computerworld, April 15, 2005, at [http://www.computerworld.com/securitytopics/security/story/0,10801,101101,00.html].

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Bank of America - computer data tapes lost during shipment	February 2005	GSA charge card program (Visa cards issued to federal employees)	1.2 million	customer and account information	Carrns, Ann, "Bank of America Is Missing Tapes With Card Data,"*Wall Street Journal*, February 28, 2005, p. B2.
Wells Fargo - computers stolen from Wells Fargo vendor	November 2004	mortgage and student-loan customers	company would not disclose	customers' names, addresses, and SSNs, and account numbers	Breyer, R. Michelle, "Wells Fargo Customer Data Stolen in Computer Theft ,"*Austin-American Statesman*, November 3, 2004, p. D1.
Wells Fargo - hacker arrested with stolen computers and laptop	November 2003	customers with personal lines of credit used for consumer loans and overdraft protection	company would not disclose	names, addresses, account and SSNs	"Suspect Is Arrested in Theft of Bank Data," *Los Angeles Times*, November 27, 2003, p. C2.
Weichert Financial Services - credit profiles were unlawfully accessed from internal computer system	May 2003	clients	3,774	credit reports, driver's license info	*Associated Press*, "Pair Accused of Fraud in Credit Reports' Theft: Allegedly Used Data to Buy Goods over the Internet,"*The Record* (Bergen County, NJ), May 2, 2003, p. A10.

Financial Institutions Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Visa, MasterCard, American Express and Discover account numbers - hacker stole 8 million	February 2003	credit card customers	PNC Bank cancelled 16,000 cards; Citizens Bank cancelled 8,000-10,000 cards	ATM/debit/check cards	Sabatini, Patricia, "PNC Cancels 16,000 Cards After Hacking Theft Incident," *Pittsburgh Post-Gazette*, February 20, 2003, p. C1.
Fullerton, California - bogus credit card ring opened bank accounts, credit lines, auto and home loans	June 2001	impersonated more than 1,500 people nationwide and defrauded 76 financial institutions	1,500	birth dates, SSNs, mothers' maiden names, credit cards, driver's licenses, and receipts for car and home purchases.	Brown, Aldrin and Jeff Collins, "Suspicious Mail Triggered Probe of Identity Theft Crime Losses from the Alleged Ring, Which Used Data Stolen as Far Back as the Early '90s, May Hit $10 Million," *Orange County Register*, June 21, 2001 (no page given).

Table 4. Data Security Breaches in State and Federal Government (2003-2006)

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
U.S. Department of Commerce - 1,137 stolen, lost, or missing laptops	September 2006	Census Bureau and National Oceanic and Atmospheric Administration	6,200 households (estimated)	unknown	Sipress, Alan, "1,100 Laptops Missing from Commerce Dept.," Washington Post, September 22, 2006, p. A3.
U. S. Department of Veterans Affairs - missing computer from contractor's office	August 2006	patients at VA hospitals in Pennsylvnia	38,000	SSNs, names, addresses, birth dates, insurance carriers, billing information, details of service	Rash, Wayne, "Another VA Computer Goes Missing," eWeek, August 7, 2006, at [http://www.eweek.com/article2/0,1895,2000268,00.asp]
U.S. Department of Transportation - stolen laptop	August 2006	drivers license records of Florida residents	133,000	SSNs, names, addresses	Rash, Wayne, "DOT is the Latest Victim of Computer Theft," eWeek, August 10, 2006, at [http://www.eweek.com/article2/0,1895,2002148,00.asp?kc=EWNAVEMNL081106EOAD]
U.S. Department of Education - exposed loan data	August 2006	students who borrowed money under the Federal Direct Student Loan program	21,000	names, birth dates, SSNs, addresses, phone numbers and in some cases account information for holders of federal direct student loans	Yen, Hope, "Ed. Dept. offers free credit monitoring," *Houston Chronicle*, August 24, 2006 (no page given).

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Naval Safety Center - personal data exposed on website and on 1,100 computer discs mailed to naval commands	July 2006	Naval and Marine Corps aviators and air crew, both active and reserve	"more than 100,000"	SSNs, personal information	"Naval Safety Center Finds Personal Data on Website," U.S. Department of Defense press release, July 8, 2006, at [http://www.news.navy.mil/search/display.asp?story_id=24568].
U.S. State Department - hackers	July 2006	Washington headquarters, and the Bureau of East Asian and Pacific Affairs	unknown	access to data and passwords	"State Department Releases Details Of Computer System Attacks," *COMMWEB*, July 13, 2006 (no page given), and Greenemeier, Larry, "State Department Hack Escalates Federal Data Insecurity," Information Week, July 12, 2006, at [http://www.informationweek.com/news/showArticle.jhtml?articleID=190302905].
Federal Trade Commission	June 2006	subjects of law enforcement investigations	110	names, addresses, SSNs, financial account numbers	*Reuters*, "FTC Laptops Stolen, 110 People at Risk of ID Theft," Baseline.com, June 23, 2006 (no page given).
U.S. Navy - an open website contained five spreadsheet files with personal information	June 2006	Navy members and dependents	30,000	names, birth dates and SSNs	"Navy Personal Data on Web Is Katrina-related," *States News Service*, June 26, 2006 (no page given).
Texas Guaranteed Student Loan- computer equipment lost	June 2006	college students borrowing money from the loan company	1.3 million	names, SSNs	Evers, Joris, "Loan Company Reports Loss of Data on 1.3 Million," CNet News, June 1, 2006, at [http://news.com.com/Loan+company+reports+loss+of+data+on+1.3+million/2100-1029_3-6079261.html].

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
National Institutes of Health Federal Credit Union (Rockville, MD)	June 2006	credit union members	"small number"	unidentified personal information	Trejos, Nancy, "Identity Thieves Hit NIH Credit Union; Scheme Is Latest in Spate of Breaches Affecting Millions," *Washington Post*, June 29, 2006, p. B3.
U.S. Department of Agriculture- external security breach of a workstation and two servers	June 2006	current and retired employees of the department	26,000	names, SSNs, employee photos, internal building locations	Azaroff, Rachel, "Hacker Might Have Breached Personal Data at USDA," *FCW*, June 22, 2006, at [http://www.fcw.com/article94991-06-22-06-Web].
Minnesota Department of Revenue (St. Paul, MN) - missing data tape	June 2006	individuals and businesses (taxpayers)	2,400 individuals and 48,000 businesses	names, addresses, SSNs, employment data	MN Department of Revenue, "Department of Revenue to Assist Taxpayers Whose Private Information Was Included in a Package Lost in the Mail," June 28, 2006, at [http://www.taxes.state.mn.us/taxes/publications/press_releases/content/taxpayer_information.shtml]
Department of Energy- file stolen by hacker	June 2006	employees of the Energy Department's nuclear weapons agency	1,500	names, SSNs, birth datess, codes showing where the employees worked, codes showing their security clearance	*Associated Press*, "DOE Computers Hacked; Info on 1,500 Taken," June 11, 2006.

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Government Accountability Office (GAO) -website exposed data from audit reports on Defense Department travel vouchers from the 1970s	June 2006	DoD employees	"fewer than 1,000"	service members' names, SSNs, addresses	Thormeyer, Rob, "GAO Removes Archived Personal Data from Web Site," WashingtonTechnology.com, June 27, 2006 at [http://www.washingtontechnology.com/news/1_1/daily_news/28845-1.html].
King County Records, Elections, and Licensing Services Division (Seattle, WA) - website exposed personal data	June 2006	current and former county residents	unknown (potentially thousands)	SSNs	*Associated Press*, "Councilman Irked by Data Postings on Web," June 27, 2006.
Internal Revenue Service - lost laptop	June 2006	IRS employees and job applicants	291	names, birth dates, SSNs, fingerprints	Lee, Christopher, "IRS Laptop Lost with Data on 291 People," *Washington Post*, June 8, 2006, p. A4.
Nebraska Treasurer's Office (Lincoln, NE) - hacker broke into a child-support computer system	June 2006	individuals and employers who pay and receive child support payments	300,000 individuals and 9,000 employers	names, SSNs, tax identification numbers for businesses	Nebraska State Treasurer, "Hacker Virus Stopped by Treasurer's Office," June 29, 2006, at [http://www.treasurer.state.ne.us/ie/server.asp]
Pentagon, Tricare Management Activity- hackers break into server	May 2006	Defense Department conference attendees	14,000	names, SSNs, credit card numbers, employer identification, other personal information	Barr, Stephen, "Conference Attendees' Personal Data May Be at Risk," *Washington Post*, May 12, 2006, p. D4.

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Department of Veterans Affairs- laptop and external hard drive stolen	May 2006	military veterans	26.5 million	names, birth dates, SSNs	Lee, Christopher and Steve Vogel, "Personal Data on Veterans is Stolen," *Washington Post*, May 23, 2006, p. A1.
National Institutes of Health (NIH)- posting of confidential grant applications	October 2005	applicants to the NIH	undisclosed	grant proposals and other grant review materials	Pulley, John L., "NIH Accidentally Posts Confidential Grant Applications on the Web," *The Chronicle of Higher Education*, October 31, 2005 (no page given).
U.S. Air Force - records stolen from the Air Force Personnel Center's online Assignment Management System	August 2005	officers and 19 NCOs	33,300	SSNs, birth dates, and other sensitive information	Dorsett, Amy, "Identity theft Threat Hangs over AF Officers," *San Antonio Express-News*, August 24, 2005, p. 1A.
San Diego County Employees Retirement Association - hackers broke into two computers	July 2005	current and retired county government employees	33,000	workers' names, Social Security numbers, addresses and dates of birth	Chacon, Daniel, "Hackers Breach County's Personal Records; 33,000 People at Risk in Retirement Association," *San Diego Union-Tribune*, July 30, 2005, p. B1.

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Federal Deposit Insurance Corporation - computer breach in early 2004. The agency wrote to employees that it learned of the breach only "recently", but did not explain how the breach occurred, aside from stating that it was not the result of a computer security failure.	June 2005	FDIC current and former employees or anyone employed at the agency as of July 2002.	6,000	names, birth dates, SSNs, and salary information	Krim, Jonathan, "FDIC Alerts Employees of Data Breach", *Washington Post*, June 16 2005, p. D1.
Lucas County (OH) Children Services - information from the agency's personnel database was compiled and e-mailed to an outside computer	June 2005	agency's 400 current employees and about 500 others who have worked there since 1991	900	names, telephone numbers, SSNs	Patch, David, "Lucas County Children Services Data Stolen," *Toledo Blade*, June 28, 2005, p. B1.
hackers breached Illinois Employment Development Department server	February 2004	people who work as domestic employees and those who employ them	90,000	SSNs, wages	"Hackers Breach State Files on 90,000," *Chicago Tribune*, February 15, 2004, p. 12.

Government (State and Federal) Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
U.S. Department of Defense - hackers downloaded Navy credit cards	August 2003	Navy's purchase card program, used to order routine office supplies	13,000	credit card numbers	Reddy, Anitha, "Hackers Steal 13,000 Credit Card Numbers; Navy Says No Fraud Has Been Noticed," *Washington Post*, November 23, 2003, p. E1.
Bronx identity theft ring filed thousands of fraudulent income tax returns	February 2003	income tax filers	not specified	SSNs **note:** ID theft ring obtained $7million in tax refunds	Weiser, Benjamin, "19 Charged in Identity Theft That Netted $7 Million in Tax Refunds," *New York Times*, February 5, 2003, p. B3.

Table 5. Data Security Breaches in Health Care (2003-2006)

Healthcare Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
Medco Health Solutions-stolen laptop	March 2006	Ohio state employees and their dependents	4,600	SSNs, birth dates	Weiss, Todd R., "Vendor Waited Six Weeks to Notify Ohio Officials of Data Breach," Computerworld, March 1, 2006, at [http://www.computerworld.com/printthis/2006/0,4814,109116,00.htm].
Children's Health Council, San Jose, California - stolen backup tape	September 2005	patients, employees, and parents of patients	5,000-6,000	psychiatric records, evaluations and SSNs; also payroll data on hundreds of current and former employees and credit card information from parents of patients	Walsh, Diana, "Data Stolen from Children's Psychiatric Center," *San Francisco Chronicle*, September 20, 2005, p. B8.
San Jose Medical Group Management - desktop computers stolen from locked administrative office	April 2005	former patients from last seven years	185,000	names, addresses, SSNs, confidential medical information	Weiss, Todd, "Update: Stolen Computers Contain Data on 185,000 Patients," Computerworld, April 8, 2005, at [http://www.computerworld.com/databasetopics/data/story/0,10801,100961,00.html].

Healthcare Incidents	Date Publicized	Who Was Affected	Number Affected	Type of Data Released/Compromised	Source(s)
TriWest Healthcare Alliance - theft of a database containing names and SSNs	December 2002	military personnel and their dependents	500,000	names, addresses, SSNs	Gorman, Tom, "Reward Offered in Huge Theft of Identity Data; Stolen Computers Had Names, Social Security Numbers of 500,000 Military Families,"*Los Angeles Times*, January 1, 2003, p. 14.

Source: The tables were prepared by CRS from publicly available and news media sources.The author would like to acknowledge the technical assistance of Carol Glover and Logan Council in preparing these tables.)

crsphpgw

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