Order Code RL33199

CRS Report for Congress
Received through the CRS Web

Personal Data Security Breaches: Context and Incident Summaries

December 16, 2005

Rita Tehan
Information Research Specialist
Knowledge Services Group

Personal Data Security Breaches: Context and Incident Summaries

Summary

Personal data security breaches are occurring 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 was the first of its kind in the nation, implemented in July 2003.

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, but to date, none have been enacted.

This report will be updated regularly.

Contents

List of Tables

Personal Data Security Breaches: Context and Incident Summaries

Introduction

Personal data security breaches are occurring 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 are not only the result of illegal or fraudulent attacks by computer hackers, but often because of careless business practices.

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 was the first of its kind in the nation, which was implemented in July 2003.

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

---

[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.privacy.ca.gov/code/cc1798.291798.82.htm] 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].

[3] 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].

An estimated 10 million consumers are affected annually by lost or stolen data at a cost to the economy of $53 billion.[4] Moreover, victims spend almost 300 million hours a year trying to clear their names and re-establish good credit ratings.[5]

Despite the growing fear of Internet related 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.[6] 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 were stolen and "account-level" breaches, where only account numbers — sometimes associated with names — were stolen. The report concludes that even in the most dangerous data breaches, where thieves access Social Security numbers and other sensitive information on consumers they have deliberately targeted, the fraud rate was 0.098% — less than one in 1,000 identities potentially revealed.[7]

Nonetheless, according to a June 2005 survey by Gartner, Inc., a technology research firm, nearly 60% of consumers said they worry more about thieves getting undetected access to private credit reports and other sensitive financial data than defending against phishing attacks.[8] Nearly one-third are "extremely concerned" that they will suffer some type of identity theft fraud because of unauthorized access to their data.[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 they are 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]

---

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

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

[6] 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].

[7] 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].

[8] 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.

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

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

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.[11] 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 an interview. "Criminals are now saying, Why am I using a gun?"[12]

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.[13] 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.[14] The FTC is also an enforcement agency and does not release data on companies while an investigation is ongoing. When there is an enforcement action, the FTC releases information identifying corporations, organization, or others who have violated data security laws.

Although a number of federal agencies (e.g., the FTC, 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 and Privacy Rights Clearinghouse are involved with data privacy investigations or consumer assistance, none maintains a comprehensive itemized list of data security breaches.

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 this year, but to date, none have been enacted. For a discussion of legislative and other issues on this topic, see CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, 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*, Marcia S. Smith.

Table 1 summarizes selected data security or identity theft breaches reported in the press since 2000. A few highlights compiled from the reported incidents:

---

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

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

[13] 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].

[14] 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].

- Almost half of the security breaches occurred at institutions of higher education. (A recent *Chronicle of Higher Education* article examines why this is so, noting that while colleges have become better at detecting electronic break-ins, security practices, particularly password protections, are lax[15]. 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[16]);

- 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

- In 2005, a stolen computer (desktop, laptop, or hard drive) was the cause of the security breach 20% of the time.

---

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

[16] 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].

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

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
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.
Georgia Institute of Technology Office of Enrollment Services - computer theft	November 2005	past, present, and prospective students	13,000	SSNs, birthdates, 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].
TransUnion (credit reporting bureau) - stolen desktop computer	November 2005	customers	3,600	SSNs and personal credit information	"Credit Bureau Burglary Leaves 3,600 Vulnerable," *Atlanta Journal and Constitution*, November 11, 2005.
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.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Indiana University - malicious software programs installed on business instructor's computer	November 2005	Kelly School of Business students enrolled in introductory business course between 2001-2005	5,300	personal student information	"IU Finds 'Malicious' Software," Associated Press, *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.
University of Tennessee - inadvertent posting of names and Social Security numbers to Internet listserv	October 2005	students and employees	1,900	names and SSNs	"State Briefs: UT Students' Private Data Posted on the 'Net," *The Tennessean.com*, October 29, 2005, at [http://tennessean.com/apps/pbcs.dll/article?AID=/20051029/NEWS01/510290327/1006/NEWS01].
Bank of America - stolen laptop	September 2005	Visa Buxx card users	undisclosed	names, credit card numbers, bank account numbers, routing transit numbers	McMillan, Robert, "Bank of America Notifying Customers After Laptop Theft," *Computerworld*, October 7, 2005, at [http://www.computerworld.com/securitytopics/security/story/0,10801,105246,00.html].

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

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Kent State University - five desktop computers stolen from campus	September 2005	students and professors	100,000	names, SSNs, grades	Gonzalez, Jennifer, "Student, Faculty Data on Stolen Computers," *Plain Dealer (Cleveland)*, September 10, 2005, p. B1.
California State University - Office of the Chancellor may have experienced unauthorized access to one of its computers	August 2005	students who receive financial aid and two financial aid administrators	154	names, SSNs	"California State University Chancellor's Office Experiences Potential Computer Security Breach,"*U.S. Fed News*, August 29, 2005.
J.P. Morgan (Dallas) - stolen laptop	August 2005	clients	unknown	personal and financial information	"Security Breach at J.P. Morgan Private Bank,"*AFX International Focus*, August 30, 2005.
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].
U.S. Air Force - records stolen from the Air Force Personnel Center's online Assignment Management System	August 2005	officers and 19 NCOs	33,300	SSNs, birthdates, and other sensitive information	Dorsett, Amy, "Identity theft Threat Hangs over AF Officers," *San Antonio Express-News*, August 24, 2005, p. 1A.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Colorado - hackers tapped into a database in the registrar's office	August 2005	student records from June 1999 to May 2001 and from fall 2003 to summer 2005.	49,000	names, SSNs, addresses, phone numbers	Mccrimmon, Katie Kerwin, "Hackers Tap CU Registrar's Database; Privacy of 49,000 Students Potentially Invaded in Breach," *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 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.
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.
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.

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

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

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

Incident	Date Publicized	Who Was Affected	No. 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 late last year at a processing center in Tucson operated by CardSystems Solutions, one of several companies that handle transfers of payment between the bank of a credit card-using consumer and the bank of the merchant where a purchase was made. CardSystems' computers were breached by malicious code that allowed access to customer data.	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].

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

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

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
New Jersey cybercrime ring stole financial records from bank accounts	May 2005	customers of four banks (Charlotte, North Carolina-based Bank of America and Wachovia, Cherry Hill, New Jersey-based Commerce Bank, and PNC Bank of Pittsburgh)	700,000	names, SSNs, bank account information **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].
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].

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
HSBC (global bank) sent out warning letters notifying customers that criminals may have gained access to credit card info	April 2005	holders of General Motors MasterCard who had shopped at Polo Ralph Lauren	180,000	credit card information	"Security 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].
San Jose Medical Group Management - desktop computers stolen from locked administrative office	April 2005	former patients from last 7 years	185,000	names, addresses, SSNs, confidential medical information	Weiss, Todd, "Update: Stolen Computers Contain Data on 185,000 Patients," *Computerworld*, April 8, 2005, at [http://www.computerworld.com/databasetopics/data/story/0,10801,100961,00.html].
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.

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

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

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of California, San Diego (UCSD) - hacker breached computer system	January 2005	students and alumni of UCSD Extension	3,500	names, SSNs	Yang, Eleanor, "Hacker Breaches Computers That Store UCSD Extension Student, Alumni Data," *San Diego Union Tribune*, January 18, 2005, p. B3.
George Mason University - hackers gained access to information	January 2005	faculty, staff, and students	30,000	names, photos, SSNs, and campus ID numbers	McCullagh, Declan, "Hackers Steal ID Info from Virginia University," *Wired News*, January 10, 2005, at [http://news.com.com/2100-7349_3-5519592.html].
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.
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.
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].

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
California State - auditor from chancellor's office lost hard drive containing personal information	August 2004	380,000 current and former students, applicants, staff, faculty and alumni at UC San Diego and 178,000 at San Diego State	23,500	name, address, SSNs	Connell, Sally Ann, "Security Lapses, Lost Equipment Expose Students to Possible ID Theft; in the Latest Incident, a Cal State Hard Drive with Data on 23,500 Individuals Is Missing," *Los Angeles Times*, August 29, 2004, p. B4.
Lowe's (home improvement store) - hacker used vulnerable wireless network to attempt to steal credit card info	June 2004	customers	unknown	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].
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].

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

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Acxiom (marketing company) - hacker downloaded data	August 2003	clients include 14 of the top 15 credit card companies, 5 of the top 6 retail banks, IBM, Microsoft, and federal government	10% of clientele (no total number given)	passwords, personal, financial, and company information	Lee, W.A. "Hacker Breaches Acxiom Data," *American Banker*, August 11, 2003, p. 5.
U.S. Department of Defense - hackers downloaded Navy credit cards	August 2003	Navy's purchase card program, used to order routine office supplies	13,000	credit card numbers	Reddy, Anitha, "Hackers Steal 13,000 Credit Card Numbers; Navy Says No Fraud Has Been Noticed," *Washington Post*, November 23, 2003, p. E1.
Weichert Financial Services - credit profiles were unlawfully accessed from internal computer system	May 2003	clients	3,774	credit reports, driver's license info	Associated Press, "Pair Accused of Fraud in Credit Reports' Theft: Allegedly Used Data to Buy Goods over the Internet,"*The Record* (Bergen County, NJ), May 2, 2003, p. A10.
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.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Texas, Austin - computer hackers broke into database on multiple occasions	March 2003	current and former student, faculty and staff members, as well as job applicants	55,200	names, addresses, SSNs, email addresses, office phone numbers **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.
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].
Visa, MasterCard, American Express and Discover account numbers - hacker stole 8 million	February 2003	credit card customers	PNC Bank cancelled 16,000 cards; Citizens Bank cancelled 8,000-10,000 cards	ATM/debit/check cards	"PNC Cancels 16,000 Cards After Hacking Theft Incident," *Pittsburgh Post-Gazette*, February 20, 2003, p. C1.
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.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
University of Kansas - hacker break-in to Student and Exchange Visitor Information System (SEVIS)	January 2003	foreign students	1,400	SSNs, passport numbers, countries of origin, and birth dates.	Arnone, Michael, "Hacker Steals Personal Data on Foreign Students at U. of Kansas,"*Chronicle of Higher Education*, January 24, 2003.
TriWest Healthcare Alliance - theft of a database containing names and SSNs	December 2002	military personnel and their dependents	500,000	names, addresses, SSNs	Gorman, Tom, "Reward Offered in Huge Theft of Identity Data; Stolen Computers Had Names, Social Security Numbers of 500,000 Military Families,"*Los Angeles Times*, January 1, 2003, p. 14.
TCI help-desk worker sold client access codes to two others, who then used the codes to obtain more than 15,000 customer credit records	November 2002	credit reporting bureau customers	15,000 (*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.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Midwest Express Airlines and Federal Aviation Administration - hackers posted list of customer names to website and posted a list of airport security screening results taken from the FAA's system	April 2002	Midwest Express Airlines customers; FAA (two separate incidents)	unknown	passenger names and airport security screening results	Larson, Virgil, "Computer Hackers Breach Midwest Express Systems," *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/].
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.
Fullerton, California - bogus credit card ring which opened bank accounts, credit lines, auto and home loans	June 2001	impersonated more than 1,500 people nationwide and defrauded 76 financial institutions	1,500	birth dates, SSNs, mothers' maiden names, credit cards, driver's licenses, and receipts for car and home purchases.	Brown, Aldrin and Jeff Collins, "Suspicious Mail Triggered Probe of Identity Theft Crime Losses from the Alleged Ring, Which Used Data Stolen as Far Back as the Early '90s, May Hit $10 Million," *Orange County Register*, June 21, 2001.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
New York City restaurant busboy duped credit reporting companies into providing detailed credit reports	March 2001	chief executives, celebrities and tycoons from Forbes list of richest Americans	200	SSNs, home addresses and birth dates, credit card numbers	Hays, Tom, "Busboy Hacks Only the Richest, Used Forbes' List in Plot to Steal Identity, Credit Info, Big Bucks," *Pittsburgh Post-Gazette*, March 21, 2001, p. A11.
World Economic Forum - hackers broke into computer	February 2001	attendees	3,200	passport numbers, cell phone numbers, credit card numbers, exact arrival and departure times, hotel names, room numbers, number of overnights, sessions attended, plus information on 27,000 people who have attended the global forum in recent years	Higgins, Alexander, "Hackers Steal World Leaders' Personal Data," *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.
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.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Egghead - hacker attacked computer system	December 2000	customers	3.5 million credit card accounts; 7500 of which showed "suspected fraudulent activity"	credit card info	"Sayer, Peter, "Egghead Says Customer Data Safe After Hack Attack," *PC World*, January 8, 2001 at [http://msn.pcworld.com/news/article/0,aid,37781,00.asp].
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 Pres, "Hacker Said to Steal 300,000 Card Numbers," *Arizona Republic*, January 11, 2000, p. A3.

Incident	Date Publicized	Who Was Affected	No. Affected	Type of Data Released/Compromised	Source(s)
Pacific Bell - 16-year-old teenager hacked into server and stole passwords	January 2000	subscribers	63,000 accounts were decrypted; 330,000 customers told to change passwords	passwords	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.

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

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