A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

DATE MADE PUBLIC	NAME (Location)	TYPE OF BREACH	NUMBER OF RECORDS
August 13, 2007	Pfizer/Axia Ltd. (New York, NY) 866-274-3891	Axia Ltd. had notified Pfizer on June 14 of an incident in which two Pfizer laptops were stolen from a locked car. The laptops, which disappeared May 31 in Boston, included the names and Social Security numbers of health-care professionals who “were providing or considering providing contract services for Pfizer,” according to the letter.	950
August 11, 2007	Providence Alaska Medical Center (Anchorage, AL) (888) 387-3392.	A laptop computer that contains the personal information of patients is missing. On the laptop there maybe names, medical record numbers, dates of birth, patient diagnoses, Social Security numbers and addresses.	250
August 10, 2007	Loyola University (Chicago, IL)	A computer with the Social Security numbers of 58 hundred students was discarded before its hard drive was erased, forcing the school to warn students about potential identify theft.	5,800
August 10, 2007	Legacy Health System (Portland, OR) (503) 445-9533	A primary care physician practice has discovered the theft of $13,000 in cash and personal data for patients. Patient receipts, credit card transaction slips and checks are also missing, in addition to Social Security numbers and dates of birth for patients.	747
August 8, 2007	Yale University (New Haven, CT)	Social Security numbers for over 10,000 current and former students, faculty and staff were compromised last month following the theft of two University computers	10,000
August 7, 2007	Electronic Data Systems (Montgomery, AL)	A former employee was arrested this week for allegedly trafficking in stolen identities she received through her work with the company. She "obtained the names and identifying information of 498 Alabama Medicaid recipients and subsequently sold 50 of those identities.	498
August 7, 2007	Merrill Lynch (Hopewell, NJ)	A computer device apparently was stolen containing sensitive personal information, including Social Security numbers, about some 33,000 employees.	33,000
August 6, 2007	Verisign (Mountain View, CA)	A laptop containing extensive personal information on an undisclosed number of VeriSign employees was stolen from an employee's car. The information included names, addresses, Social Security numbers, dates of birth, telephone numbers, and salary records.	Unknown
August 4, 2007	Kellogg Community Federal Credit Union (Battle Creek, MI)	A computer containing personal information on an undisclosed number members was stolen. A file containing some members' names, addresses, telephone numbers, birth dates, Social Security numbers and account numbers was on the computer's hard drive.	Unknown
August 3, 2007	WorkCare Orem (Pleasant Grove, UT)	A truck driver found medical documents containing personal information in his truck and on the ground while he picked up a load at a garbage transfer station. The documents contained names, addresses, telephone numbers, Social Security numbers and birth dates.	Unknown
August 3, 2007	Wabash Valley Correctional Facility (Indianapolis, IN)	A database containing Social Security numbers, dates of birth and names of people employed at the facility between 1997 and 2002 was unintentionally moved “from a secure private drive that was accessible only by the human resources department to a shared directory that could be accessed by other employees here.”	Unknown
August 2, 2007	E.On - U.S.(energy services) (Louisville, KY)	A laptop with names, Social Security numbers and birth dates of most E.On U.S. employees and some retirees was stolen last month.	Unknown
August 2, 2007	University of Toledo (Toledo, OH) (419) 530-4836 (419) 530-3661 (419) 530-1472	A computer was stolen with two hard drives containing student and staff Social Security numbers, names, and grade change information.	Unknown
August 1, 2007	Lifetime Fitness (Dallas, TX)	Staff had discarded customer records in easily accessible trash cans behind the businesses. Information that was discarded contained names, addressed, Social Security numbers and credit card information, as well as the date of birth of several children.	Unknown

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

July 28, 2007	Yuba County Health and Human Services (Yuba County, CA)	A laptop stolen from a building contained personally identifiable information of individuals whose cases were opened before May 2001. The laptop was being used as a backup system for the county's computer system. The data include Social Security numbers, birth dates, driver's license numbers and other private information.	70,000
July 27, 2007	Flexible Benefits Administrators (Virgina Beach VA)	A former employee allegedly stole Virginia Beach city and school district employees' personal information and used it to commit prescription fraud. Police discovered a list of names and Social Security numbers at the employees home.	2,000
July 27, 2007	City Harvest (New York, NY) (917) 351-8763	City Harvest is currently investigating a potential improper access of systems that contained credit card information of their donors.	12,000
July 27, 2007	American Education Services (Harrisburg, PA)	Personal information was on a laptop stolen in a burglary at a subcontractor's headquarters. The information, which was not encrypted, included names, addresses, phone numbers, e-mail addresses and Social Security numbers.	5,000
July 26, 2007	United States Marine Corps / Penn State University (Harrisburg, PA)	Names and Social Security numbers of Marines were found through Google Internet search engine.	10,554
July 25, 2007	Hidalgo County Commissioner's Office (Hidalgo County, TX)	The private medical information, including Social Security numbers and treatment details of people who sought medical assistance from the county was posted on the Hidalgo County Website.	25
July 24, 2007	St. Vincent Hospital (Indianapolis, IN)	A security lapse compromised names, addresses and Social Security numbers.	51,000
July 23, 2007	Fox News	A security hole on the Fox News web server Sunday exposed sensitive content to the public, including login information that allowed hackers to access names, phone numbers, and email addresses of at least 1.5 million people	Not added to total, it does not appear that SSNs or financial account numbers were exposed.
July 21, 2007	University of Michigan (Ann Arbor, MI)	University databases were hacked. Names, addresses, Social Security numbers, birth dates, and in some cases, the school districts where former students were teaching were exposed.	5,500
July 20, 2007	SAIC (San Diego, CA) www.saic.com/response/ (703) 676-6533	Pentagon contractor may have compromised personal information. Information such as names, addresses, birth dates, Social Security numbers and health information about military personnel and their relatives because it did not encrypt data transmitted online.	580,000
July 19, 2007	Cricket Communications	Documents stolen from store result in loss of 300 credit card numbers.	300
July 19, 2007	Jackson Local Schools (Massillon, OH)	The Social Security numbers of present and former Jackson Local Schools' employees were at risk of public access on a county maintained Web site.	1,800
July 18, 2007	Purdue University (West Lafayette, IN) (866) 605-0013	Files which were no longer in use were discovered on a computer server connected to the Internet. The files contained names and Social Security numbers of students who were enrolled in an industrial engineering course.	50
July 18, 2007	Connecticut General Assembly Transportation Committee (Hartford, CT)	Social Security numbers of former employees of defunct L.G. Defelice Inc. posted on CT transportation committee website.	300
July 17, 2007	Western Union (Greenwood Village, CO)	Credit card information and names were hacked from a database.The thieves got names, addresses, phone numbers and complete credit-card information.	20,000
July 17, 2007	Louisiana Board of Regents (Baton Rouge, LA)	Records of students and staff including Social Security numbers,names, and addresses exposed on web.In all, more than 80,000 names and Social Security numbers were accessible for perhaps as long as two years on an internal Internet site.	80,000
July 17, 2007	Kingston Technology Co.	Security breach that remained undetected until "recently" may have compromised the names, addresses	27,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	(Fountain Valley, CA)	and Credit Card details of online customers.	
July 16, 2007	Prudential Financial Inc. (Newark, NJ)	Data exposed in the breach was faxed to a company by doctors and clinics across the U.S.. Data included the patients' Social Security numbers, bank details and health care information.	1,000
July 16, 2007	TSA (Arlington, VA)	Authorities realized in May a storage device was missing from TSA headquarters. The drive contained historical payroll data, Social Security numbers, dates of birth, addresses, time and leave datas, bank account, routing information, and details about financial allotments and deductions.	100,000
July 15, 2007	Westminster College (Salt Lake City, UT)	Names of students, former and current were printed in two files along with each student's Social Security number. The files were on a student Web server used by Westminster students.	100
July 13, 2007	City of Encinitas (Encinitas, CA) (760) 633-2788	Credit card or checking account information and addresses of people who had enrolled in Encinitas' youth recreation programs was inadvertently posted on the city's Web site.	1,200
July 13, 2007	Metropolitan St. Louis Sewer District (St.Louis, MO)	A employee had downloaded Social Security numbers of current or former district employees to a home computer. The Social Security numbers were part of a computer file the district uses to make sure workers get the proper pay.	1,600
July 11, 2007	South County Hospital (South Kingstown, RI)	Paperwork containing personal details from customers was left in a briefcase inside a car that was stolen. That batch of paperwork contained details including names, addresses, Social Security numbers, phone numbers and a summary of hospital accounts.	79
July 11, 2007	Texas A&M University (College Station, TX)	College of Business officials are investigating a faculty member for the misplacement of a business law class roster containing the names and Social Security numbers of students.	49
July 11, 2007	Disney Movie Club / Alta Resources (Neenah, WI)	A contract employee stole an unknown number of credit card numbers. Credit-card information was sold by an employee of a Disney contractor to a federal agent as part of an undercover sting operation.	Unknown
July 9, 2007	Girl Scouts Mile Hi (Denver CO) (303) 778-8774	Tapes stolen from a car held personal information from a membership database, including names, addresses, phone numbers. A very limited number of credit card numbers and Social Security numbers were included in the stolen data from the camp and event registration database.	Unknown
July 7, 2007	Cuyahoga County Dept. of Development (Cleveland, OH)	Names and Social Security numbers on memory stick stolen in carjacking.	3,000
July 5, 2007	Highlands University (Las Vegas, NM)	A building on the campus had been broken into, and the affected offices might have had such personal information as Social Security numbers, credit card and bank account information exposed.	420
July 3, 2007	Fidelity National Information Services Certegy Check Services Inc. St. Petersburg, FL)	A worker at one of the company's subsidiaries (Certegy Check Services, Inc.) stole customer records containing credit card, bank account and other personal information.	2.300,000
June 29, 2007	Harrison County Schools (Charleston WV)	Several computers that contained the personal information, including Social Security numbers, of several Harrison County school employees were stolen. Workers Comp claims between January of 2001 and February of 2007 are at risk.	Unknown
June 27, 2007	Milwaukee PC (Milwaukee, WI) (414) 258-2275	Credit card information for 65,000 was possibly compromised. A service center noticed a file in their server and was concerned that file could contain customers' credit card numbers and personal information.	65,000
June 27, 2007	Bowling Green State University (Bowling Green, OH)	Lost storage device contained Social Security numbers, and names of 199 former students.	199
June 27, 2007	University of California, Davis (Davis, CA) www.vetmed.ucdavis.edu/computer_security deansoffice@vetmed.ucdavis.edu (530) 752-8032.	Computer-security safeguards were breached and accessed information including the applicants' names, birth dates and, in most cases, Social Security numbers.	1,120

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

June 25, 2007	Fresno County (Fresno, CA) (559) 453-6450	A disk containing information pertaining to home health-care workers -- including their names, addresses and Social Security numbers was lost.	Unknown
June 23, 2007	Winn-Dixie (Pascagoula,MS)	Pharmacy documents were found behind closed Winn-Dixie, containing telephone numbers, Social Security numbers and addresses of thousands. Apparently when they closed up, they put these bundles outside to be picked up and they were never picked up.	Unknown
June 22, 2007	Texas First Bank (Texas City, TX)	Information such as account numbers, Social Security numbers, names and addresses may have been stored on a stolen laptop computer during a car theft in Dallas.	4,0000
June 20, 2007	American Airlines (Fort Worth, TX)	Personal information including Social Security numbers of pilots and other employees at American Airlines, including the chief executive, was exposed on a company Web site.	365
June 20, 2007	University Community Hospital (Tampa, FL)	A parent says his son should never have received bills in the mail for a pre-employment drug screening visit. Among the bills there's something else he was surprised to see, information about others who were also tested, "Like 17 of them here with the Social Security numbers."	Unknown
June 18, 2007	Parisexposed.com (Bellevue, WA)	Investigation by The Smoking Gun Web site said that by changing a few characters on the web page URL it was possible to see the subscriber's name, email address, password, phone number, mailing address and credit card number.	750
June 18, 2007	Shamokin Area School District (Coal Township, PA)	A local newspaper employee gained unauthorized access to the Shamokin Area School District's computer database. It is the same system that stores students' personal information, including Social Security numbers. That newspaper employee brought the security flaw to the attention of school officials.	Unknown
June 18, 2007	Texas A&M University (College Station, TX)	A professor vacationing off the coast of Africa took data with him on a small computer, which was lost or stolen. It is thought to contains SSNs and dates of birth for students enrolled in the spring, summer and fall semesters of 2006	8,000
June 15, 2007	Ohio state workers (Columbus, OH) (888) 644-6648 (taped-message) (877) 742-5622 (Ohio Consumers' Counsel) or (800) 267-4474	A backup computer storage device with the names and Social Security numbers of every state worker was stolen out of a state intern's car. **UPDATE** (6/20/07) : The storage device also had the names and Social Security numbers of 225,000 taxpayers, **UPDATE** (6/22/07) : Previous news stories reported smaller amounts, but the most recent news story shows 500,000 .	500,000
June 14, 2007	Division of Workforce Services (Salt Lake City, Utah) (801) 281-1267	Children's Social Security numbers are believed to have been compromised by identity thieves.	20,000
June 14, 2007	Hamburger Hamlet Restaurant (Los Angeles CA)	Former waitress made off with the credit or debit card numbers of at least half a dozen patrons - and possibly as many as 40. Already, about $16,300 in unauthorized charges have been linked to the scam.	40
June 14, 2007	Georgia Tech Univ. (Atlanta, GA)	An electronic file containing the personal information of current and former Georgia Tech students was exposed briefly.	23,000 (not included in Total because it's not clear SSNs or account numbers were exposed).
June 14, 2007	Lynchburg City (Lynchburg, VA) (434) 455-3964 IDsupport@lynchburgva.gov	Personal information of Lynchburg city employees and retirees was accidentally posted on the city's website among that information employee's prescription medications.	1,200 (not included in Total because it's not clear SSNs or account numbers were exposed).
June 11, 2007	Pfizer (New York, NY)	Installation of certain file sharing software on a Pfizer laptop, exposed files containing names, Social Security numbers, addresses and bonus information of present and former Pfizer colleagues.	17,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	866-274-3891	Investigation revealed that certain files containing data were accessed and copied.	
June 11, 2007	Grand Valley State University (Allendale, MI) Jann Joseph (616) 331-2110	A flash drive containing confidential information was stolen. Social Security numbers of current and former students were on the flash drive, stolen from the English department.	3,000
June 9, 2007	Concord Hospital (Concord NH) mhanna@cmonitor.com	Names, addresses, dates of birth and Social Security numbers exposed on the internet "for a period of time,"security lapsed from a subcontractor that handles its online billing. **UPDATE** (6/20/07): Washington-based company that was managed its online billing system was fired. Hospital officials now are asking for an audit to verify that Verus Incorporated has removed all of its patient information from its servers.	9,000
June 8, 2007	University of Virginia (Charlottesville, VA) identity-assistance@virginia.edu (866) 621-5948	A breach in one of the computer applications that resulted in exposure of sensitive information belonging to current and former U.Va. faculty members. The information included names, Social Security numbers and dates of birth. The investigation has revealed that on 54 separate days between May 20, 2005 and April 19, 2007, hackers tapped into the records of 5,735 faculty members.	5,735
June 8, 2007	University of Iowa www.grad.uiowa.edu/news/incident.htm (Iowa City, IA)	Social Security numbers of faculty, students and prospective students were stored on the Web database program that was compromised.	1,100
June 7, 2007	Huntsville County Huntsville, AL	As many as 400 people and banking institutions may be victims in a credit card or debit card cloning. In Alabama and Georgia card numbers were stolen after the cards were used at Huntsville restaurants and carry-out businesses.	400
June 6, 2007	Cedarburg High School (Cedarburg, Wisconsin)	Students obtained names, addresses and Social Security numbers and might have accessed personal bank account information of current and former district employees..	Unknown
June 6, 2007	Dearfield Medical Building (Greenwich, CT)	A box was discovered at inside a trash bin in May and contains information about lab tests and insurance approvals as well as other medical issues, documents are not medical charts, but do contain patient names and contact information.	Unknown
June 6, 2007	HarborOne Credit Union (Brockton, Mass.)	Data compromise disclosed by the retailer in January. The breach resulted in HarborOne having to block and reissue about 9,000 debit cards.	9,000
June 4, 2007	Stevens Hospital (Edmonds, WA) (425) 673-3745	Laptop exposed to Internet, information did include names, addresses, and Social Security numbers.The situation occurred when one of the subcontractors had a lapse in its data security procedures.	550
June 3, 2007	Gadsden State Community College (College Gadsden, AL)	Students who took an Art Appreciation class at the Ayers Campus between 2005 and 2006 had their names, grades and Social Security numbers scattered across a local business' driveway.	400
June 1, 2007	Fresno County/Refined Technologies Inc. (Fresno, CA)	Missing computer disk contains names, addresses, Social Security numbers.The county sent it by courier to a software vendor's office in San Jose to determine workers' eligibility for health care benefits.The software company, Refined Technologies Inc., said they never received the disk.	10,000
June 1, 2007	Jax Federal Credit Union (Jacksonville, FL)	Social Security numbers and account numbers of clients were accidentally posted on the Internet, then indexed by Google. JFCU was transmitting information to a printer for a preapproved auto loan mailing when the information was picked up by Google from the printer's Web site. JFCU normally transmits information on an encrypted disk delivered by courier, but when the printer couldn't open the disk, the information was sent again, but wasn't encrypted and included Social Security numbers and account numbers.	7,766
June 1, 2007	Northwestern University (Evanston,Ill) c-loebbaka@northwestern.edu (847) 491-4887	Files containing personal information of students and applicants were available online.	4,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

May 31, 2007	Priority One Credit Union (South Pasadena, CA)	Priority One Credit Union sent out election ballots to members with Social Security numbers and account numbers printed on the outside of the envelopes	Unknown
May 26, 2007	Cover Tennessee (Nashville, Tenn.)	A computer error at the Cover Tennessee health insurance program caused small business owners who chose not to print out their forms from the Web site to have their personal information including Social Security numbers added to the next user's printout request.	279
May 25, 2007	North Carolina Dept. of Transportation (Raleigh, NC)	A computer server used to back up employee identification badge records that included the names and Social Security numbers of NCDOT employees, contractors and other state employees was compromised.	25,000
May 25, 2007	Booker T. Washington Community Center (Auburn, NY)	A laptop computer with personal information of individuals who applied for Family Health Plus or Child Health Plus state health insurance program benefits was recovered when a woman tried to sell it at a pawn shop.	Unknown
May 24, 2007	Beacon Medical Services (Aurora, CO)	Private medical and financial information including patient records from at least 10 Colorado clinics and hospitals, and one hospital in Peoria, Illinois that should have been only accessible through VPN access were inadvertently available on the Internet.	5,000
May 23, 2007	Waco Independent School District (Waco, TX)	Two high school seniors recently hacked into the district's computer network potentially compromising the personal information including Social Security numbers of students and employees.	17,400
May 23, 2007	Check into Cash (Champaign, IL)	Consumer loan documents and related reports were found in a trash bin behind the shopping center where Check into Cash is located. Documents contained Social Security numbers, addresses, copies of driver's licenses and other personal information of the company's customers.	Unknown
May 22, 2007	University of Pittsburgh Medical Center (Pittsburgh, PA)	UPMC mailed a fundraising letter to 6,000 former patients on May 7. The donor response cards "inadvertently" included each individual's SSN in the tracking code, visible through the envelope window.	6,000 former patients
May 22, 2007	University of Colorado-Boulder (Boulder, CO) www.colorado.edu Hotline: (303) 492-1655	A hacker launched a worm that attacked a University computer server used by the College of Arts and Sciences. Information for 45,000 students enrolled at UC-B from 2002 to the present was exposed, including SSNs. The breach was discovered May 12. Apparently anti-virus software had not been properly configured.	45,000 students
May 21, 2007	Columbia Bank (Fair Lawn, NJ)	Columbia Bank notified its online banking customers of a hacking incident. Names and SSNs were accessed, but account numbers and passwords were not.	Unknown
May 20, 2007	Northwestern University financial aid office (Chicago, IL)	A laptop belonging to the financial aid office was stolen. It contained SSNs and other information of "some alumni."	Unknown
May 19, 2007	Texas Commission on Law Enforcement Standards and Education (Austin, TX)	A computer was stolen from the state agency that licenses police officers. It contained information on every licensed peace officer in Texas, including SSNs, driver's license numbers, and birth dates.	230,000
May 19, 2007	Illinois Dept. of Financial and Professional Regulation (Chicago, IL) For information about breach, www.idfpr.com For information about ID theft, www.illinoisattorneygeneral.gov	A computer server in the office of the Illinois Dept. of Financial and Professional Regulation was breached earlier this year. SSNs, tax numbers, and addresses of banking and real estate professionals were exposed. The hacking incident was discovered May 3.	300,000 licensees and applicants
May 19, 2007	Stony Brook University (Stony Brook, NY) www.stonybrook.edu/disclosure Call Center, (866) 645-5830 (available until July 15, 2007)	SSNs and university ID numbers of faculty, staff, students, alumni, and other community members were visible via the Google search engine after they were posted to a Health Sciences Library Web server April 11. It was discovered and removed 2 weeks later.	90,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

May 18, 2007	Alcatel-Lucent (Murray Hill, NJ)	The telecom and networking equipment maker notified employees that a computer disk containing personal information was lost in transit to Aon Corp., another vendor. It contained names, addresses, SSNs, birth dates, and salary information of current and former employees.	Unknown
May 18, 2007	Yuma Elementary School District No. 1 (Yuma, AZ)	SSNs of 91 substitute teachers were stolen May 7 when a district employee's car was broken into and a brief case was taken containing payroll reports. The reports did not include bank account information..	91
May 18, 2007	Indianapolis Public Schools (Indianapolis, IN)	A local newspaper reporter discovered that sensitive personal information was accessible online, including employee performance reviews, student gradebooks, student special education needs, and essays	7,500 students [not included in Total because it is not clear if SSNs were exposed]
May 17, 2007	Detroit Water and Sewerage Department (Detroit, MI)	A laptop containing City employee information was stolen from the vehicle of an insurance company employee .	3,000 (not included in Total below because it is not known if the data included SSNs)
May 17, 2007	Georgia Div. of Public Health (statewide)	The GA Dept. of Human Resources notified parents of infants born between 4/1/06 and 3/16/07 that paper records containing parents' SSNs and medical histories -- but not names or addresses -- were discarded without shredding.	140,000
May 15, 2007	IBM (Armonk, NY)	An unnamed IBM vendor lost computer tapes containing information on IBM employees -- mostly ex-workers -- including SSNs, dates of birth, and addresses. They went missing in transit frm a contractor's vehicle.	Unknown
May 15, 2007	San Diego Unified School District (San Diego, CA) H.R. Services Division Identity Theft Hotline: (619) 725-8086, operational through June 1, 2007, 8am to 5pm, M-F	In a letter to its employees, the School District said it had been notified by law enforcement that a former employee had access to personal identification information of "a select number of district employees." Those employees were notified separately. The letter said it has "no specific knowledge of any attempted fraud..."	Unknown
May 14, 2007	Community College of Southern Nevada (North Las Vegas, NV)	A virus attacked a computer server and could have allowed a hacker to access students' personal information including names, Social Security numbers and dates of birth, but the school is not certain whether anything was actually stolen from the school's computer system.	197,000
May 12, 2007	Goshen College (Goshen, IN) info@goshen.edu (866) 877-3055	A hacker accessed a college computer that contained the names, addresses, birth dates, Social Security numbers and phone numbers of students and information on some parents with the suspected motivation of using the system to send spam e-mails.	7,300
May 12, 2007	Doctor and dentist (Leon Valley, TX)	A local TV news reporter exposed that a medical office disposed of patient records without shredding them. Included were SSNs and dates of birth, as well as medical information.	Unknown
May 11, 2007	Univ. Calif. Irvine Medical Center (Irvine, CA)	About 1,600 file boxes stored in an off-site university warehouse were discovered missing. Some of the files included patients' names, addresses, Social Security numbers and medical record numbers.	287
May 11, 2007	Highland Hospital (Rochester, NY) HighlandHospitalAdmin@urmc.rochester.edu www.stronghealth.com/ (866) 917-5034	Two laptop computers, one containing patient information including Social Security numbers, were stolen from a business office. The computers were sold on eBay, and the one containing personal information was recovered.	13,000
May 8, 2007	Univ. of Missouri (Columbia, MO) (866) 241-5619	A hacker accessed a computer database containing the names and Social Security numbers of employees of any campus within the University system in 2004 who were also current or former students of the Columbia campus.	22,396
May 7, 2007	Indiana Dept. of Administration (Indianapolis, IN)	An employee uploaded a list of certified women and minority business enterprises to the department's Web site and inadvertently included their tax identification numbers, which for some businesses and sole	"dozens" to "no more than a couple hundred"

		proprietorships is the owner's Social Security number.	
May 5, 2007	Transportation Security Administration	A computer hard drive containing payroll data from January 2002 to August 2005 including employee names, Social Security numbers, birth dates, bank account and routing information of current and former workers including airport security officers and federal air marshals was stolen. **UPDATE** (5/14/07); The American Federation of Government Employees is suing the TSA for the loss of the hard drive. It calls the breach a violation of the Privacy Act.	100,000
May 3, 2007	Maryland Dept. of Natural Resources (Annapolis, MD)	Personal information of current and retired employees including names and Social Security numbers was downloaded to a "thumb drive" by an employee who wanted to work at home but was lost en route.	1,433
May 3, 2007	Louisiana State Univ., E.J. Ourso College of Business (Baton Rogue, LA)	A laptop stolen from a faculty member's home contained personally identifiable information including may have included students' Social Security numbers, full names and grades of University students.	750
May 3, 2007	Montgomery College	A new employee posted the personal information of all graduating seniors including names, addresses and Social Security numbers on a computer drive that is publicly accessible on all campus computers.	Unknown
May 1, 2007	Healing Hands Chiropractic (Sterling, CO)	Medical records containing the personal information of chiropractic patients including records Social Security numbers, birth dates, addresses and, in some cases, credit card information wee thrown in a dumpster “due to lack of office space.”	"Hundreds"
May 1, 2007	J. P. Morgan (New York, N.Y.)	Documents containing personal financial data of customers including names, addresses and Social Security numbers were found in garbage bags outside five branch offices in New York.	Unknown
May 1, 2007	Maine State Lottery Commission (Hallowell, ME)	Documents containing personal information such as names, Social Security numbers, references to workers compensation claim records, psychiatric and other medical records, and police background checks were found in a dumpster.	Unknown
May 1, 2007	Champaign Police Officers (Champaign, IL)	The names and Social Security numbers of Champaign police officers were left on a computer donated to charity.	139
May 1, 2007	J. P. Morgan (Chicago, IL)	A computer tape containing personal information of wealthy bank clients and some employees was delivered to a secure off-site facility for storage but was later reported missing.	47,000
Apr. 29, 2007	Univ. of New Mexico (Alburquerque, NM)	Employees' personal information including names, e-mail and home addresses, UNM ID numbers and net pay for a pay period for staff, faculty and a few graduate students may have been stored on a laptop computer stolen from the San Francisco office of an outside consultant working on UNM's human resource and payroll systems.	[3,000] (Not included in Total below because SSNs were apparently not compromised)
Apr. 28, 2007	Couriers on Demand (Dallas, TX)	Personal information of job applicants was accidentally published to the Internet.	"Hundreds"
Apr. 27, 2007	Google Ads (Mountain View, CA)	Top sponsored Google ads linked to 20 popular search terms were found to install a malware program on users' computers to capture personal information and used to access online accounts for 100 different bank.	Unknown
Apr. 27, 2007	Caterpillar, Inc. (Peoria, IL)	A laptop computer containing personal data of employees including Social Security numbers, banking informatoin and addresses was stolen from a benefits consultant that works with the company.	Unknown
Apr. 26, 2007	Ceridian Corp. (Minneapolis, MN)	A former employee had data containing the personal information of employees including "ID" and bank-account data and then, accidentally posted it on a personal Web site.	150
Apr. 25, 2007	Neiman Marcus Group (Dallas, TX) (800) 456-7019	Computer equipment in the possession of a pension consultant containing files with sensitive information including name, address, Social Security number, date of birth, period of employment and salary information of Neiman Marcus Group's current and former employees and their spouses was stolen.	160,000
Apr. 24, 2007	Baltimore County Dept. of Health (Baltimore, MD)	A laptop containing personal information including names, date of birth, Social Security numbers, telephone numbers and emergency contact information of patients who were seen at the clinic between Jan. 1, 2004 and April 12 was stolen.	6,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

April 24, 2007	Purdue Univ. (West Lafayette, IN) (866) 307-8513	Personal information including names and Social Security numbers of students who were enrolled in a freshman engineering honors course was on a computer server connected to the Internet that had been indexed by Internet search engines and consequently was available to individuals searching the Web.	175
Apr. 23, 2007	Fed. Emergency Management Agency (FEMA) Washington, DC	Social Security numbers of Disaster Assistance Employees were printed on the outside address labels of . reappointment letters	2,300
Apr. 21, 2007	Albertsons (Save Mart Supermarkets) (Alameda, CA) (510) 337-8340	Credit and debit card numbers were stolen using bogus checkout-line card readers resulting in card numbers processed at those terminals being captured and some to be misused.	81
Apr. 20, 2007	Los Alamos National Laboratory (Alburquerque, NM)	The names and Social Security numbers of lab workers were posted on a Web site run by a subcontractor working on a security system.	550
Apr. 20, 2007	U.S. Agriculture Dept. (Washington, DC)	The Social Security numbers of people who received loans or other financial assistance from two Agriculture Department programs were disclosed since 1996 in a publicly available database posted on the Internet.	37,000
Apr. 19, 2007	New Mexico State Univ. (Las Cruces, NM)	The names and Social Security numbers of students who registered online to attend their commencement ceremonies from 2003 to 2005 were accidentally posted on the school's Web site when an automated program moved what was supposed to be a private file into a public section of the Web site.	5,600
Apr. 18, 2007	Ohio State Univ. (Columbus, OH)	A hacker accessed the names, Social Security numbers, employee ID numbers and birth dates of 14,000 current and former staff members. In a separate incident, the names, Social Security numbers and grades of 3,500 former chemistry students were on class rosters housed on two laptop computers stolen from a professor's home in late February.	17,500
Apr. 18, 2007	Univ. of CA, San Francisco (San Francisco, CA) (866) 485-8777 www.ucsf.edu/alert	A computer file server containing names, contact information, and Social Security numbers for study subjects and potential study subjects related to studies on causes and cures for different types of cancer was stolen from a locked UCSF office. For some individuals, the files also included personal health information.	3,000
Apr. 15, 2007	CVS Pharmacy (Liberty, TX)	The Attorney General of Texas filed a complaint against CVS Pharmacy for illegally disposing of personal information including active debit and credit card numbers, complete with expiration dates and medical prescription forms with customer's name, address, date of birth, issuing physician and the types of medication prescribed. The information was found in a dumpster behind a store that apparently was being vacated.	"hundreds"
Apr. 12, 2007	Bank of America (Charlotte, NC)	A laptop containing personal information of current, former and retired employees including names, addresses, dates of birth and Social Security numbers was stolen when an employee was a "victim of a recent break-in."	"limited" number of people
Apr. 12, 2007	Univ. of Pittsburgh, Med. Center (Pittsburgh, PA)	Personal information including names, Social Security numbers, and radiology images of patients were previously included in two medical symposium presentations that were posted on UPMC's Web site. Though the presentation was later removed in 2005, the presentations were apparently inadvertently re-posted on the site and only recently removed again.	88
Apr. 12, 2007	GA Secretary of State (Atlanta, GA)	30 boxes of Fulton County voter registration cards that contain names, addresses and Social Security numbers were found in a trash bin.	75,000
Apr. 11, 2007	New Horizons Community Credit Union (Denver, CO)	A laptop computer that contained personal information of members who had loans with the credit union was stolen from Protiviti, a consultant employed by Bellco Credit Union conducting due diligence to prepare a possible acquisition bid.	9,000
Apr. 11, 2007	ChildNet (Ft. Lauderdale, FL)	An organization responsible for managing Broward County's child welfare system believe a dishonest former employee stole a laptop from the agency's office. It contains personal information of adoptive and foster-care parents including financial and credit data, Social Security numbers, driver's license data and	12,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

		passport numbers.	
Apr. 11, 2007	Black Hills State Univ. (Spearfish, SD) (605) 642-6215	Names and Social Security numbers of scholarship winners were inadvertently posted and publicly available on the university's web site.	56
Apr. 10, 2007	Georgia Dept. of Community Health (Atlanta, GA) (866) 213-3969	A computer disk containing personal information including addresses, birthdates, dates of eligibility, full names, Medicaid or children's health care recipient identification numbers, and Social Security numbers went missing from a private vendor, Affiliated Computer Services (ACS), contracted to handle health care claims for the state.	2,900,000
Apr. 9, 2007	Turbo Tax	Using Turbo Tax online to access previous returns, a Nebraska woman was able to access tax returns for other Turbo Tax customers in different parts of the country. The returns contained personal information needed to e-file including bank account numbers with routing digits and Social Security numbers.	Unknown
Apr. 6, 2007	Hortica (Edwardsville, IL) (800) 851-7740 securedata@hortica-insurance.com	A locked shipping case of backup tapes containing personal information including names, Social Security numbers, drivers' license numbers, and bank account numbers is missing.	Unknown
Apr. 6, 2007	Chicago Public Schools (Chicago, IL) (773) 553-1142	Two laptop computers contain the names and Social Security numbers of current and former employees was stolen from Chicago Public Schools headquarters.	40,000
Apr. 5, 2007	DCH Health Systems (Tuscaloosa, AL)	An encrypted disc and hardcopy documents containing retirement benefit information including Social Security numbers and other personal information were lost. Tracking data indicates the package was delivered to the addressee's building, but the intended recipient never received the package.	6,000
Apr. 5, 2007	Security Title Agency (Phoenix, AZ)	Hackers defamed the company's Web site and may have accessed customer information which is stored on the same server as the site.	Unknown
Apr. 4, 2007	UC San Francisco (San Francisco, CA) (415) 353-8100) isecurity@ucsf.edu http://oaais.ucsf.edu/notice	An unauthorized party may have accesed the personal information including names, Social Security numbers, and bank account numbers of students, faculty, and staff associated with UCSF or UCSF Medical Center over the past two years by compromising the security of a campus server.	46,000
Mar. 30 2007	Los Angeles County Child Support Services (Los Angeles, CA)	Three laptops containing personal information including about 130,500 Social Security numbers — most without names, 12,000 individuals' names and addresses, and more than 101,000 child support case numbers were apparently stolen from the department's office.	243,000
Mar. 30, 2007	Naval Station San Diego's Navy College Office (San Diego, CA) (866) U-ASK-NPC CSCMailbox@navy.mil	Three laptops were reported missing that may contain Sailors' names, rates and ratings, Social Security numbers, and college course information. The compromise could impact Sailors and former Sailors homeported on San Diego ships from January 2003 to October 2005 and who were enrolled in the Navy College Program for Afloat College Education.	Unknown
Mar. 30, 2007	Univ. of Montana - Western (Dillon, MT)	A computer disk containing students' Social Security numbers, names, birth dates, addresses and other personal information was stolen from a professor's office. The stolen information belonged to students enrolled in the TRIO Student Support Services program, which offers financial and personal counseling and other assistance.	400
Mar. 28, 2007	RadioShack (Portland, TX)	20 boxes of discarded records including sales receipts with credit card numbers spanning from 2001 to 2005 and personal information of store employees were found in a dumpster. UPDATE (04/03/07): The Texas Attorney General's Office filed an action against the Radio Shack store for violating the state's violating the 2005 Identity Theft Enforcement and Protection Act.	Unknown

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Mar. 28, 2007	TJX Companies -- TJ Maxx and Marshalls	See initial Jan. 17, 2007 posting for updated numbers and summary of breach information -- 45.7 million credit and debit card numbers and 455,000 customer return records.	See 1/17/07 posting
Mar. 27, 2007	St. Mary Parish (Centerville, LA)	Personal information including Social Security numbers of St. Mary Parish public school employees was available on the Internet when a Yahoo!Web crawler infiltrated the server of the school's technology department.	380
Mar. 26, 2007	Fort Monroe (Fort Monroe, VA)	A laptop computer containing the names, Social Security numbers and payroll information for as many as 16,000 civilian employees was stolen from an employee's personal vehicle. Bank account and bank routing information were not included.	16,000
Mar. 23, 2007	Group Health Cooperative Health Care System (Seattle, WA)	Two laptops containing names, addresses, Social Security numbers and Group Health ID numbers of local patients and employees have been reported missing.	31,000
Mar. 23, 2007	Swedish Urology Group (Seattle, WA)	Three computer hard drives with personal files on hundreds of local patients including was stolen.	"hundreds"
Mar. 20, 2007	Health Resources, Inc. (Evansville, IN)	From Jan 24, 2007 to Feb 6, 2007, a Web site glitch allowed employers with access to private health information to obtain the name, address, Social Security number, dependent names and birthdates of other patients.	2,031
Mar. 20, 2007	Tax Service Plus (Santa Rosa, CA)	Thieves stole the company's backup computer, which contained financial data on thousands of tax returns dating back three years.	4,000
Mar. 19, 2007	Science Applications International Corp. (SAIC) (Boise, ID)	Barrels filled with thousands of sensitive documents including printed copies of e-mail and performance evaluations along with documents marked “internal use only – not for public release” and “for official use only” were found on the curb outside of SAIC's local office.	Unknown
Mar. 16, 2007	Ohio State Auditor (Springfield, OH) www.spr.k12.oh.us Click on Notification of Data Theft	A laptop containing personal information of current and former employees of Springfield City Schools including their names and Social Security numbers was stolen from a state auditor employee's vehicle while parked at home in a garage.	1,950
Mar. 14 2006	Buffalo Bisons and Choice One Online (Buffalo, NY)	Hacker accessed sensitive financial information including credit card numbers names, passwords of customers who ordered items online.	Unknown
Mar. 14, 2007	Wellpoint's Empire Blue Cross and Blue Shield unit in NY (Indianapolis, IN) 800-293-3443	An unencrypted disc containing patient's names, Social Security numbers, health plan identification numbers and description of medical services back to 2003 was lost en route to a subcontractor. **UPDATE** (3/14/07): The subcontrator reported that the CD that was reported missing on Feb. 9 has been found.	75,000
Mar. 13, 2007	U.S. Dept. of Agriculture (Washington, D.C.)	A total of 95 USDA computers were lost or stolen between Oct. 1, 2005, and May 31, 2006. Some may have contained personal information such as names, addresses, Social Security numbers and payment information. Two-thirds of the computers contained unencrypted data.	Unknown
Mar. 12, 2007	Dai Nippon (Tokyo, Japan)	A former contract worker of a Japanese commercial printing company stole nearly 9 million pieces of private data on customers from 43 clients. The stolen data includes confidential information such as names, addresses and credit card numbers intended for use in direct mailing and other printing services. Customers of U.S.-based American Home Assurance Co. and Toyota Motor were affected.	Unknown
Mar. 10, 2007	University of Idaho (Moscow, ID) www.vandalidentity.net 888-900-3783	A data file posted to the school's Web site contained personal information including names, birthdates and Social Security numbers of University employees.	2,700
Mar. 9, 2007	California National Guard (Sacramento, CA)	A computer hard drive containing Social Security numbers, home addresses, birth dates and other identifying information of California National Guard troops deployed to the U.S.-Mexico border was	1,300

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

		stolen.	
Mar. 7, 2007	Los Rios Community College (Northern Calif.)	Student information including Social Security numbers were accessible on the Internet after the school used actual data to test a new onine application process in October.	2,000
Mar. 7, 2007	U.S. Census Bureau (Washington, D.C.)	Personal information of 302 households including names, addresses, phone numbers, birth dates and family income ranges were posted on a public Internet site multiple times over a five-month period from October 2006 to Feb. 15, 2007 when Census employees working from home tested new software records.	302 households
Mar. 3, 2007	Metropolitan State College of Denver (Denver, CO) 866-737-6622	A faculty member's laptop computer that contained the names and Social Security numbers of former students was stolen from its docking station on campus.	988
Mar. 3, 2007	Johnny's Selected Seeds (Winslow, ME)	Hacker accessed credit card account information of online customers. About 20 credit cards have been used fraudulently.	11,500
Mar. 2, 2007	Calif. Dept. of Health Services (Sacramento, CA)	Benefit notification letters containing names addresses, Medicare Part D plan names and premium payment amounts of some individuals enrolled in the California AIDS Drug Assistance Program (ADAP) were mailed to another enrollee.	54
Mar. 1, 2007	Westerly Hospital (Westerly, RI)	Patient names, Social Security numbers, contact information as well as insurance information were posted on a publicly-accessible Web site.	2,242
Feb. 28, 2007	Gulf Coast Medical Center (Nashville, TN & Tallahassee, FL)	Patient information including names and Social Security numbers was compromised when two computers went missing. 1,900 individuals were affected by a theft in Nashville, TN in November and 8,000 when another computer was stolen in Tallahassee in February.	9,900
Feb. 23, 2007	Rabun Apparel Inc., former subsidiary of Fruit of the Loom (Rabun Gap, GA)	Names and Social Security numbers of former employees were accessible on the Internet from Jan. 15 until Feb. 20.	1,006
Feb. 22, 2007	Speedmark (Woodlands, TX)	Thieves stole several computers, one of which contained a database with personally identifying information including names, addresses, e-mail accounts, and Social Security numbers of Speedmark's mystery shopper employees and contractors.	35,000
Feb. 21, 2007	Georgia Institute of Technology (Atlanta, GA) 404-894-2499 hr@gatech.edu	Personal information of former employees mostly in the School of Electrical and Computer Engineering including names, addresses, Social Security number, other sensitive information, and about 400 state purchasing card numbers was compromised by unauthorized access to a Georgia Tech computer account.	3,000
Feb. 20, 2007	Back and Joint Institute of Texas (San Antonio, TX)	20 boxes containing Social Security numbers, photocopies of driver's license numbers, addresses, phone numbers and private medical history of chiropractic patients were found in a dumpster.	"hundreds"
Feb. 19, 2007	Seton Healthcare Network (North Austin, TX)	A laptop with uninsured patients' names, birth dates and Social Security numbers was stolen last week from the Seton hospital system. The uninsured patients had gone to Seton emergency rooms and city health clinics since July 1, 2005.	7,800
Feb. 19, 2007	Clarksville-Montgomery County middle and high schools (Clarksville, TN)	Staff and faculty Social Security numbers, used as employee identification numbers, were embedded in file photos by the company that took yearbook pictures and inadvertently placed in a search engine on school system's Web site.	633
Feb. 19, 2007	Stop & Shop Supermarkets (Rhode Island and Southern MA) 877-366-2668	Credit and debit card account information including PIN numbers was stolen by high-tech thieves who apparently broke into checkout-line card readers and PIN pads and tampered with them.	Unknown
Feb. 19, 2007	Social Security Admin. (Milwaukee, WI)	Files of disability applicants containing Social Security numbers, addresses, phone numbers of family members, dates of birth and work history, and detailed medical information were lost/stolen when a telecommuting employee abandoned them in a locked filing cabinet at home after a threat of domestic violence. Several of the files were mailed back to the local SSA office months later; others were found in	13

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

		a dumpster recently, and four were never recovered.	
Feb. 15, 2007	City College of San Francisco (San Francisco, CA) (800) 436-0108 www.ccsf.edu	Names, grades, and SSNs were posted on an unprotected Web site after summer session in 1999. CCSF stopped using SSNs as studens IDs in 2002.	11,000 students
Feb. 14, 2007	Kaiser Medical Center (Oakland, CA) (866) 529-0779	A doctor's laptop was stolen from the Medical Center containing medical information of 22,000 patients. But only 500 records contained SSNs.	22,000 patients, but apparently only 500 records contained SSNs (the latter number is included in total below)
Feb. 14, 2007	Iowa Dept. of Education	Up to 600 files of G.E.D. recipients were viewed when the online database was hacked. Files included names, addresses, birthdates, and SSNs of G.E.D. graduates from 1965 to 2002.	600
Feb. 14, 2007	Conn. Office of the State Comptroller (Hartford, CT)	Personal information of state employees including names and Social Security numbers was inadvertently posted on the Internet in a spreadsheet of vendors used by the state.	1,753
Feb. 10, 2007	Official Indiana State Web site www.IN.gov (888) 438-8397 Email: securityconcerns @www.IN.gov	A hacker gained access to the State Web site and obtained credit card numbers of individuals who had used the site's online services and gained access to Social Security numbers for 71,000 health-care workers. **UPDATE** (3/22/07): Investigators have identified a teen they believe hacked into the IN.gov as a prank.	5,600 individuals and businesses and 71,000 health-cae workers
Feb. 9, 2007	East Carolina University (Greenville, NC) www.ecu.edu/incident/ 877-328-6660	A programming error resulted in personal information of 65,000 individuals being exposed on the University's Web site. The data has since been removed. Included were names, addresses, SSNs, and in some cases credit card numbers.	65,000 students, alumni, and staff members
Feb. 9, 2007	Radford University, Waldron School of Health and Human Services (Radford, VA)	A computer security breach exposed the personal information, including SSNs, of children enrolled in the FAMIS program, Family Access to Medical Insurance Security.	2,400 children
Feb. 8, 2007	Piper Jaffrey (Minneapolis, MN)	W-2s sent to current and former employees in January included employees' Social Security numbers on the outside of the envelope. Though the numbers were not identified as Social Security numbers, they followed the standard XXX-XX-XXXX format. Executives indicated the mishap was an error by a third-party vendor.	"more than 1,000 employees"
Feb. 8, 2007	St. Mary's Hospital (Leonardtown, MD)	A laptop was stolen in December that contained names, SSNs, and birthdates for many of the Hospital's patients.	130,000
Feb. 7, 2007	University of Nebraska (Lincoln, NE)	An employee accidentally posted SSNs of 72 students, professors, and staff on UNL's public Web site where they remained for 2 years. They have since been removed.	72
Feb. 7, 2007	Johns Hopkins University and Johns Hopkins Hospital (Baltimore, MD)	Johns Hopkins reported the disappearance of 9 backup computer tapes containing personal information of employees and patients, Eight of the tapes contained payroll information on 52,000 past and present employees, including SSNs and in some cases bank account numbers. The 9th tape contained "less sensitive" information about 83,000 hospital patients.	52,000 past and present employees plus 83,000 patients
Feb. 7, 2007	Front Range Ski Shop (Denver, CO)	The shop's Web site was broken into and customer information including credit card account data may have been accessed.	15,000 customers
Feb. 7, 2007	A Toronto, Ontario, residence (Canada)	Credit card data for more than 35,000 individuals from across North America were discovered by police when they executed a search warrant at a Toronto residence. A man has since been arrested on fraud and counterfeiting charges.	The number is not included in the total below because it is not known how many of the

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

			affected individuals are from the U.S.
Feb. 7, 2007	Central Connecticut State University (New Britain, CT)	Social Security numbers of about 750 CCSU students were exposed in the name and address window on envelopes mailed to them. The envelopes were not folded correctly. They contained IRS 1098T forms.	750 students
Feb. 6, 2007	NY Dept. of Labor (Glenn Falls, NY)	Laptop computer containing personal information for people who were employed by 13 Capital Region businesses stolen from state tax auditor's apartment.	537
Feb. 6, 2007	Metro Credit Services (Hurst, TX)	Files of the defunct bill collection company containing medical records, phone bills and Social Security numbers were found in a trash bin.	"thousands"
Feb. 3, 2007	CTS Tax Service (Cassopolis, MI)	The computer and hard drive of a tax preparation company were stolen. Data included names, bank account numbers, routing numbers, birthdates, SSNs, and addresses.	800
Feb. 2, 2007	Massachusetts Dept. of Industrial Accidents (Boston, MA) (800) 323-3249 ext. 560 www.mass.gov/dia	A former state contractor allegedly accessed a workers' compensation data file and stole personal information, including SSNs. The thief used the data to commit identity theft on at least 3 individuals.	1,200 people who submitted claims
Feb. 2, 2007	Indian Consulate via Haight Ashbury Neighborhood Council recycling center (San Francisco, CA)	Visa applications and other sensitive documents were accessible for more than a month in an open yard of a recycling center. Information included applicants' names, addresses, phone numbers, birthdates, professions, employers, passport numbers, and photos. A sampling of documents indicated that the paperwork included everyone who applied in the Western states from 2002-2005. Applicants were current and former executives of major Bay Area companies that have operations in India.	Unknown
Feb. 2, 2007	Wisconsin Assembly (Madison, WI)	A document containing personal information of Wisconsin Assembly members was stolen from a legislative employee's car while she was exercising at a local gym. It contained names, addresses, and SSNs.	109 Assembly members and aides
Feb. 2, 2007	University of Missouri, Research Board Grant Application System (Columbia, MO)	A hacker broke into a UM computer server mid-January and might have accessed personal information, including SSNs, of 1,220 researchers on 4 campuses. The passwords of 2,579 individuals might also have been exposed.	3,799
Feb. 2, 2007	New York Dept. of State (Albany, NY)	The agency's Web site posted commercial loan documents that mistakenly contained SSNs. The forms are posted to let lenders know the current financial status of loan recipients.	Unknown
Feb. 2, 2007	U.S. Dept. of Veteran's Affairs, VA Medical Center (Birmingham, AL) (877) 894-2600	An employee reported a portable hard drive stolen or missing that might contain personal information about veterans including Social Security numbers. **UPDATE** (2/10/07): VA increases number of affected veterans to 535,000, included in the total below. **UPDATE** (2/12/07): VA reported that billing information for 1.3 million doctors was also exposed, including names and Medicare billing codes, not included in the total below. **UPDATE** (3/19/07): The VA's Security Operations Center has referred 250 incidents since July 2006 to its inspector general, which has led to 46 separate investigations. **UPDATE** (6/18/07):More than $20 million to respond to its latest data breach, the breach potentially puts the identities of nearly a million physicians and VA patients.	48,000 veterans plus 535,000
Jan. 29, 2007	Mendoza College of Business, Notre Dame University (Notre Dame, IN, South Bend, IN)	A file of individuals who took the GMAT test (Graduate Management Admissions Test) was mistakenly left on a computer that was decommissioned. The computer was later reactivated and plugged into the Internet. Its files were available through a file-sharing program. Data included names, scores, SSNs and demographic information from 2001.	Unknown
Jan. 26, 2007	Indiana Dept. of Transportation (Indianapolis, IN)	The names and SSNs of INDOT employees were inadvertently posted on an internal network computer drive sometime between Sept. 6 and Dec. 4, 2006.	4,000 employees
Jan. 26, 2007	Vanguard University (Costa Mesa, CA) (800) 920-7312	On Jan. 16, 2 computers were discovered stolen from the financial aid office. Data included names, SSNs, dates of birth, phone numbers, driver's license numbers, and lists of assets.	5,015 financial aid applicants for 2005-2006 and 2006-2007 school years

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	www.identityalert. vanguard.edu		
Jan. 26, 2007	WellPoint's Anthem Blue Cross Blue Shield (Virginia) (800) 284-9779	Cassette tapes containing customer information were stolen from a lock box held by one of its vendors. Data included names and SSNs.	196,000 customers
Jan. 26, 2007	Chase Bank and the former Bank One, now merged (Shreveport, LA)	A Bossier woman bought a used desk from a furniture store. She discovered a 165-page spread sheet in a drawer that included names and SSNs of bank employees. The document was returned to the bank.	4,100 current and former employees "from all over Louisiana"
Jan. 26, 2007	Eastern Illinois University (Charleston, IL)	A desktop computer was stolen from the Student Life office containing membership rosters -- including SSNs, birthdates, and addresses -- of the University's 23 fraternities and sororities. A hard drive and memory from 2 other computers were also stolen.	1,400 currently enrolled students
Jan. 25, 2007	Clay High School (Oregon, OH)	A former high school student obtained sensitive staff and student information through an apparent security breach. The data was copied onto an iPod and included names, birth dates, SSNs, addresses, and phone numbers.	Unknown
Jan. 25, 2007	Ohio Board of Nursing (Columbus, OH)	The agency's Web site posted names and SSNs of newly licensed nurses twice in the past 2 months. SSNs were supposed to have been removed before posting.	3,031 newly licensed nurses
Jan. 25, 2007	Washiawa Women, Infants and Children program (WIC) (Honolulu, HI) (808) 586-8080 www.hawaii.gov	A WIC employee apparently stole the personal information of agency clients, including SSNs, and committed identity theft on at least 3 families and perhaps 2 more. The Health Director said the agency will no longer use SSNs in its data base.	11,500 current and former clients
Jan. 23, 2007	Rutgers-Newark University, Political Science Dept. (Newark, NJ)	An associate professor's laptop was stolen, containing names and SSNs of 200 students. Rutgers no longers uses SSNs as student IDs, but student IDs from past years are still SSNs.	200 students
Jan. 22, 2007	U.S. Dept. of Veteran's Affairs (Seattle, WA)	Folders of veterans' personal information were stolen from a locked car in Bremerton, WA. News stories are not clear on the type of information contained in the folders.	Unknown
Jan. 22, 2007	Chicago Board of Elections (Chicago, IL)	About 100 computer discs (CDs) with 1.3 million Chicago voters' SSNs were mistakenly distributed to aldermen and ward committeemen. CDs also contain birth dates and addresses.	1.3 million voters
Jan. 19, 2007	U.S. Internal Revenue Service via City of Kansas City (Kansas City, MO)	26 IRS computer tapes containing taxpayer information were reported missing after they were delivered to City Hall. They potentially contain taxpayers' names, SSNs, bank account numbers, or employer information. The 26 tapes were the entire shipment received by the City last August. The disappearance was noticed late December 2006.	Unknown
Jan. 18, 2007	KB Home (Charleston, SC)	A computer was stolen from one of the home builder's offices. It likely contained names, addresses, and SSNs of people who had visited the sales office for Foxbank Plantation in Berkeley County near Charleston.	2,700
Jan. 17, 2007	TJ stores (TJX), including TJMaxx, Marshalls, Winners, HomeSense, AJWright, TKMaxx, and possibly Bob's Stores in U.S. & Puerto Rico -- Winners and HomeGoods stores in Canada -- and possibly TKMaxx stores in UK and Ireland (Framingham, Mass.) U.S.: Call (866) 484-6978 Canada: (866) 903-1408	The TJX Companies Inc.experienced an "unauthorized intrusion" into its computer systems that process and store customer transactions including credit card, debit card, check, and merchandise return transactions. It discovered the intrusion mid-December 2006. Transaction data from 2003 as well as mid-May through December 2006 may have been accessed. According to its Web site, TJX is "the leading off-price retailer of apparel and home fashions in the U.S. and worldwide." **UPDATE** (2/22/07): TJX said that while it first thought the intrusion took place from May 2006 to January 2007, it now thinks its computer system was also hacked in July 2005 and on "various subsequent dates" that year. **UPDATE** (3/21/07): Information stolen from TJX's systems was being used fraudulently in November 2006 in an $8 million gift card scheme, one month before TJX officials said they learned of the breach,	45,700,000 credit and debit card account numbers 455,000 merchandise return records containing customer names and driver's license numbers

	U.K. & Ireland: 0800 77 90 15 www.tjx.com	according to Florida law enforcement officials. **UPDATE** (3/29/07): The company reported in its SEC filing that 45.7 million credit and debit card numbers were hacked, along with 455,000 merchandise return records containing customers' driver's license numbers, Military ID numbers or Social Security numbers. **UPDATE** (4/22/07): Initially, TJX said the break-in started seven months before it was discovered. Then, on Feb. 18, the company noted the perpetrators had access to data for 17 months, and apparently began in July 2005. **UPDATE** (04/26/07): Three states' banking associations (MA, CT, and ME) filed a class action lawsuit against TJX to recover the costs of damages totaling "tens of millions of dollars" incurred for replacing customers' debit and credit cards. **UPDATE** (05/04/07): An article in the WSJ notes that because TJX had an outdated wireless security encryption system, had failed to install firewalls and data encryption on computers using the wireless network, and had not properly install another layer of security software it had bought, thieves were able to access data streaming between hand-held price-checking devices, cash registers and the store's computers. 21 U.S. and Canadian lawsuits seek damages from the retailer for reissuing compromised cards. **UPDATE** (07/10/07): U.S. Secret Service agents found TJX customers' credit card numbers in the hands of Eastern European cyber thieves who created high-quality counterfeit credit cards. Victims are from the U.S., Europe, Asia and Canada, among other places, Several Cuban nationals in Florida were arrested with more than 200,000 credit card account numbers.	
Jan. 17, 2007	Rincon del Diablo Municipal Water District (Escondido, CA, plus unincorporated neighborhoods outside the city, and parts of San Marcos and San Diego, CA) (760) 745-5522	2 computers were stolen from the district office. One included names and credit card numbers of customers.	500 customers
Jan. 16, 2007	University of New Mexico (Albuquerque, NM)	At least 3 computers and 4 monitors were stolen from the associate provost's office overnight between Jan. 2 and 3. They may have included faculty members' names and SSNs.	Unknown
Jan. 13, 2007	North Carolina Dept. of Revenue (Raleigh, NC)	A laptop computer containing taxpayer data was stolen from the car of a NC Dept. of Revenue employee in mid-December. The files included names, SSNs or federal employer ID numbers , and tax debt owed to the state.	30,000 taxpayers
Jan. 12, 2007	MoneyGram International (Minneapolis, MN)	MoneyGram, a payment service provider, reported that a company server was unlawfully accessed over the Internet last month. It contained information on about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers.	79,000
Jan. 11, 2007	University of Idaho, Advancement Services office (Moscow, ID) (866) 351-1860 www.identityalert.uidaho.edu	Over Thanksgiving weekend, 3 desktop computers were stolen from the Advancement Services office containing personal information of alumni, donors, employees, and students. 331,000 individuals may have been exposed, with as many as 70,000 records containing SSNs, names and addresses.	70,000
Jan. 10, 2007	University of Arizona (Tucson, AZ)	Breaches occurred in November and December 2006 that affected services with UA Student Unions, University Library, and UA Procurement and Contracting Services. Some services were shut down for several days.	Unknown
Jan. 9, 2007	Altria, the parent company of Philip Morris (Kraft Foods), also United Technologies, via benefits consultant, Towers Perrin. (New York, NY)	5 laptops were stolen from Towers Perrin, allegedly by a former employee. The theft occurred Nov. 27, 2006. The computers contain names, SSNs, and other pension-related information, presumably of several companies, although news reports are not clear. **UPDATE** (1/11/07): NY police arrested "a junior-level administrative employee" of the company in the theft of the laptops.	18,000 past and present employees, presumably of Altria (total number of affected invididuals is unknown)

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Jan. 5, 2007	Dr. Baceski's office, internal medicine (Somerset, PA)	A hard drive was stolen containing personal information on "hundreds of patients."	"hundreds of patients"
Jan. 4, 2007	Selma, NC, Water Treatment Plant (Johnston County, NC)	A laptop stolen from the water treatment facility holds the names and SSNs of Selma volunteer firefighters.	Unknown
Jan. 4, 2007	Unnamed medical center, via Newark Recycling Center (Stockton, CA)	An individual found unshredded medical records in 36 boxes at the Newark Recycling Center.	Unknown
Jan. 2, 2007	Deaconess Hospital (Evansville, IN)	A computer missing from the hospital holds personal information, including SSNs, of 128 respiratory therapy patients.	128 patients
Jan. 2, 2007	Notre Dame University (Notre Dame, IN, South Bend, IN)	A University Director's laptop was stolen before Christmas. It contained personal information of employees, including names, SSNs, and salary information.	Unknown
Jan. 2, 2007	News accounts are not clear as to source, but thought to be a realty office (Las Vegas, NV)	About 40 boxes of financial paperwork, thought to be from loan applications, was found in a dumpster. One of the boxes visible to news reporters was said to contain paperwork with bank account details, photocopies of driver's licenses, SSNs and "other private information."	Unknown
Jan. 1, 2007	Wisconsin Dept. of Revenue via Ripon Printers (Madison, WI) (608) 224-5163 www.privacy.wi.gov	Tax forms were mailed to taxpayers in which SSNs were inadvertently printed on the front of some Form 1 booklets. Some were retrieved before they were mailed.	171,000 taxpayers
Dec. 30, 2006	KeyCorp (Cleveland, OH)	A laptop computer stolen from a KeyCorp vendor contains personally identifiable information, including SSNs, of 9,300 customers in six states.	9,300
Dec. 28, 2006	U.S. State Department	A bag containing approximately 700 completed passport applications was reported missing on December 1. The bag, which was supposed to be shipped to Charlotte, NC, was found later in the month at Los Angeles International Airport.	700 (not included in total)
Dec. 27, 2006	Montana State University (Bozeman, MT)	A student working in the loan office mistakenly sent packets containing lists of student names, Social Security numbers, and loan information to other students	259 students
Dec. 22, 2006	Texas Woman's University (Dallas, Denton, and Houston, TX)	A document containing names, addresses and SSNs of 15,000 TWU students was transmitted over a non-secure connection.	15,000 students
Dec. 21, 2006	Santa Clara County employment agency (Santa Clara County, CA)	A computer stolen from the agency holds the SSNs of approximately 2,500 individuals.	2,500
Dec. 20, 2006	Lakeland Library Cooperative - serving 80 libraries in 8 counties (Grand Rapids, MI)	Personal information of 15,000 library users in West Michigan was displayed on the Cooperative's Web site due to a technical problem. Information exposed included names, phone numbers, e-mail addresses, street addresses, and library card numbers. Children's names were also listed along with their parents' names on a spreadsheet document. The information has since been removed.	15,000 library users
Dec. 20, 2006	Big Foot High School (Walworth, WI)	Personal information was accidentally exposed on the High School's Web site for a short time, perhaps for about 36 minutes, according to a report. Information included last names, SSNs, and birthdates.	87 current and former employees
Dec. 20, 2006	Lake County residents, plus Major League Baseball players (Northbrook, IL)	A Chicago man apparently removed documents from a trash bin outside SFX Baseball Inc., a sports agency that deals with Major League Baseball. He used information found on those documents to commit identity theft on at least 27 Lake County residents. Information found during a search of the thief's home included SSNs, birthdates, canceled paychecks, obituaries, and infant death records.	27 residents of Lake County plus about 90 current and retired Major League Baseball players for a total of 117 individuals
Dec. 20, 2006	Deb Shops, Inc. (Philadelphia, PA) (800) 460-9704	A hacker illegally accessed company Web pages and a related data base used for Internet-based purchases. The intruder may have accessed customers' credit card information including names on cards and credit card numbers.	Unknown
Dec. 19, 2006	Mississippi State University	SSNs and other personal information were "inadvertently" posted on a publicly accessible MSU Web site.	2,400 students and

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	(Jackson, MS)	The breach was discovered "last week" and the information has since been removed.	emplolyees
Dec. 15, 2006	University of Colorado - Boulder, Academic Advising Center (Boulder, CO) www.colorado.edu	A server in the Academic Advising Center was the subject of a hacking attack. Personal information exposed included names and SSNs for individuals who attended orientation sessions from 2002-2004. CU-Boulder has since ceased using SSNs as identifiers for students, faculty, staff, and administrators.	17,500
Dec. 15, 2006	City of Wickliffe (Wickliffe, OH)	Hackers breached security in one of the city's three computer servers containing personal information on some city employees, including names and SSNs.	125 employees
Dec. 14, 2006	Electronic Registry Systems affecting Emory University (Emory Hospital, Emory Crawford Long Hospital, Grady Memorial Hospital), Geisinger Health System (Pennyslvania), Williamson Medical Center (Nashville, TN)	On Nov. 23, 2006, two computers (one desktop, one laptop) were stolen from Electronic Registry Systems, a business contractor in suburban Springdale, OH, that provides cancer patient registry data processing services. It contained the personal information (name, date of birth, Social Security number, address, medical record number, medical data and treatment information) of cancer patients from hospitals in Pennsylvania , Tennessee , Ohio and Georgia , dating back to 1977 at some hospitals. **UPDATE** (1/14/07): The number of affected patients was increased from 25,000 to 63,000.	More than 63,000 patients
Dec. 14, 2006	Riverside High School (Durham, NC)	Two students discovered a breach in the security of a Durham Public Schools computer as part of a class assignment. They reported to school officials that they were able to access a database containing SSNs and other personal information of thousands of school employees. The home of one student was searched by Sheriff's deputies and the family computer was seized.	"thousands of school employees"
Dec. 14, 2006	St. Vrain Valley School District (Longmont, CO)	Paper records containing student information were stolen, along with a laptop, from a nurse's car Nov. 20. Personal information included students' names, dates of birth, names of their schools, what grade they are in, their Medicaid numbers (presumably SSNs), and their parents' names. The laptop contained no personal data.	600 students
Dec. 14, 2006	Bank of America (Charlotte, NC)	A former contractor for Bank of America unauthorizedly accessed the personal information (name, address, phone number, Social Security number) of an undisclosed number of customers, for the purpose of committing fraud.	Unknown
Dec. 13, 2006	Boeing (Seattle, WA)	In early December, a laptop was stolen from an employee's car. Files contained names, salary information, SSNs, home addresses, phone numbers and dates of birth of current and former employees. **UPDATE** (12/14/06): Boeing fired the employee whose laptop was stolen. **UPDATE** (1/26/07): The laptop was recovered.	382,000 current and former employees
Dec. 13, 2006	The 100 million mark was reached Dec. 13, 2006.	Click here for a news story in IDG about this dubious milestone. And read Poulsen and Singel in Wired Blogs. Here is an article from VNUnet, and another from Washington Post. Read also the NY Times and GovExec. The **major source** for the breaches reported in this list is the list-serve and web site of Attrition.org.	**Please note**: The number refers to *records,* NOT persons. Many individuals have experienced more than one breach. For a commentary by PogoWasRight on this matter, click here.
Dec. 12, 2006	University of California - Los Angeles (Los Angeles, CA) Affected individuals can call UCLA at (877) 533-8082. www.identityalert.ucla.edu	Hacker(s) gained access to a UCLA database containing personal information on current and former students, current and former faculty and staff, parents of financial aid applicants, and student applicants, including those who did not attend. Exposed records contained names, SSNs, birth dates, home addresses, and contact information. About 3,200 of those notified are current or former staff and faculty of UC Merced and current and former staff of UC's Oakland headquarters.	800,000
Dec. 12, 2006	University of Texas - Dallas (Dallas, TX) Affected individuals can call (972) 883-4325	The University discovered that personal information of current and former students, faculty members, and staff may have been exposed by a computer network intrusion -- including names, SSNs, home addresses, phone numbers and e-mail addresses. **UPDATE** (12/14/06): The number of people affected was first thought to be 5,000, but was increased to	35,000 current and former students, faculty, staff, and others

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	www.utdallas.edu/datacompromise/form.html	6,000. **UPDATE** (01/19/07): Officials now say 35,000 individuals may have been exposed.	
Dec. 12, 2006	Aetna / Nationwide / Wellpoint Group Health Plans via Concentra Preferred Systems (Dayton, OH)	A lockbox holding personal information of health insurance customers was stolen Oct. 26. Thieves broke into an office building occupied by insurance company vendor, Concentra Preferred Systems. The lockbox contained computer backup tapes of medical claim data for Aetna and other Concentra health plan clients. Exposed data includes member names, hospital codes, and either SSNs or Aetna member ID numbers. SSNs of 750 medical professionals were also exposed. Officials downplay the risk by stating that the tapes cannot be used on a standard PC. **UPDATE** (12/23/06): The lockbox also contained tapes with personal information of 42,000 NY employees insured by Group Health Insurance Inc.) **UPDATE** (1/24/07): Personal data of 28,279 Nationwide's Ohio customers were also compromised.	130,000 plus 42,000 reportedlater plus 28,279 reported later
Dec. 9, 2006	Virginia Commonwealth University (Richmond, VA)	Personal information of 561 students was inadvertently sent as attachments on Nov. 20 in an e-mail, including names, SSNs, local and permanent addresses and grade-point averages. The e-mail was sent to 195 students to inform them of their eligibility for scholarships.	561 students
Dec. 8, 2006	Segal Group of New York, via web site of Vermont state agency used to call for bids on state contracts (Montpelier, VT)	Names and SSNs of "several hundred" physicians, psychologists and other health care providers were mistakenly posted online by Segal Group, a contractor hired by the state to put its health management contract out for bid. The information was posted from May 12 to June 19. It was discovered when a doctor found her own SSN online.	"several hundred, likely more" health care providers **UPDATE** (1/14/07): SSNS of "more than 1,100 doctors, psychothereapists and other health professionals" were exposed.
Dec. 6, 2006	Premier Bank (Columbia, MO, with HQ in Jefferson City, MO)	A report was stolen the evening of Nov. 16 from the car of the bank's VP and CFO while employees were celebrating an award received by the bank. The document contained names and account numbers of customers, but reportedly no SSNs.	1,800 customers
Dec. 5, 2006	Army National Guard 130th Airlift Wing (Charleston, WV)	A laptop was stolen from a member of the unit while he was attending a training course. It contained names, SSNs, and birth dates of everyone in the 130th Airlift Wing.	Unknown
Dec. 5, 2006	Nassau Community College (Garden City, NY)	A printout is missing that contans information about each of NCC's 21,000 students, including names, SSNs, addresses, and phone numbers. It disappeared from a desk in the Student Activities Office.	21,000 students
Dec. 5, 2006	H&R Block	Many past and present customers received unsolicited copies of the program TaxCut that displayed their SSN on the outside.	Unknown
Dec. 3, 2006	City of Grand Prairie (Grand Prairie, TX)	Employees of the city of Grand Prairie were notified that personal records were exposed on the city's Web site for at least a year. Included were the names and SSNs of "hundreds of employees." The information has since been removed. The city had been working with a contractor on a proposal for workers' compensation insurance. Along with the proposal, names and SSNs were mistakenly listed.	"hundreds of employees"
Dec. 2, 2006	Gundersen Lutheran Medical Center (LaCrosse, WI)	A Medical Center employee used patient information, including SSNs and dates of birth, to apply for credit cards in their names. As patient liaison, her duties included insurance coverage, registration, and scheduling appointments. She was arrested for 37 counts of identity theft, and was convicted of identity theft and uttering forged writing, according to the criminal complaint.	unknown
Dec. 1, 2006	TD Ameritrade (Bellevue, NE) (201) 369-8373	According to a letter sent to employees, a laptop was removed (presumably stolen) from the office Oct. 18, 2006, that contained unencrypted information including names, addresses, birthdates, and SSNs.	about 300 current and former employees
Nov. 30, 2006	Pennsylvania Dept. of Transportation (Hanover township driver's license facility, Dunmore, PA) Affected individuals can call (800) PENNDOT if you have questions.	Thieves stole equipment from a driver's license facility late evening Nov. 28, including computers containing personal information on more than 11,000 people. Information included names, addresses, dates of birth, driver's license numbers and both partial and complete SSNs (complete SSNs for 5,348 people). Also stolen were supplies used to create drivers licenses and photo IDs. The state maintains 97 driver's license facilities.	11,384

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	Call PA Crimestoppers if you have tips, (800) 4PATIPS, reward offered.		
Nov. 30, 2006	TransUnion Credit Bureau via Kingman, AZ, court office	Four different scam companies downloaded the credit information of more than 1,700 individuals, including their credit histories and SSNs. They were able to illegitimately obtain the password to the TransUnion account held by the Kingman, AZ, court office, which apparently has a subscription to the bureau's services.	"more than 1,700 people"
Nov. 28, 2006	Kaiser Permanente Colorado -- its Skyline and Southwest offices (Denver, CO) For members who have questions: (866) 529-0813.	A laptop was stolen from the personal car of a Kaiser employee in California on Oct. 4. It contained names, Kaiser ID number, date of birth, gender, and physician information. The data did not include SSNs.	38,000 (not included in total, because SSNs were apparently not exposed)
Nov. 28, 2006	Cal State Los Angeles, Charter College of Education (Los Angeles, CA) (800) 883-4029	An employee's USB drive was inside a purse stolen from a car trunk. It contained personal information on 48 faculty members and more than 2,500 students and applicants of a teacher credentialing program. Information included names, SSNs, campus ID numbers, phone numbers, and e-mail addresses.	2,534
Nov. 27, 2006	Johnston County, NC	Personal data, including SSNs, of thousands of taxpayers, were inadvertently posted on the county web site. The information was removed from the site within an hour after officials became aware of the situation.	Unknown
Nov. 27, 2006	Greenville County School District (Greenville, SC)	School district computers sold to the WH Group at auctions between 1999 and early 2006 contained the birth dates, SSNs, driver's license numbers and Department of Juvenile Justice records of approximately 100,000 students. The computers also held sensitive data for more than 1,000 school district employees. **UPDATE** (12/10/06): A judge ordered the WH Group to return the computers and the confidential data on them to the school district.	At least 101,000 students and employees
Nov. 27, 2006	Chicago Public Schools via All Printing & Graphics, Inc. (Chicago, IL)	A company hired to print and mail health insurance information to former Chicago Public School employees mistakenly included a list of the names, addresses and SSNs of the nearly 1,740 people receiving the mailing. Each received the 125-page list of the 1,740 former employees.	1,740 former Chicago Public School employees
Nov. 25, 2006	Indiana State Department of Health via Family Health Center of Clark County (Jeffersonville, IN)	Two computers stolen from an Indiana state health department contractor contained the names, addresses, birth dates, SSNs and medical and billing information for more than 7,500 women. The data were collected as part of the state's Breast and Cervical Cancer Program.	7,700
Nov. 20, 2006	Administration for Children's Services (New York , NY)	More than 200 case files from the Emergency Children's Services Unit of ACS were found on the street in a plastic garbage bag. The files contain sensitive information of families, social workers and police officers.	200 case files (not included in Total because it is not clear if SSNs were exposed)
Nov. 17, 2006	Jefferson College of Health Sciences (Roanoke, VA)	An email containing the names and SSNs of 143 students intended for one employee was inadvertently sent to the entire student body of 900.	143
Nov. 17, 2006	Automatic Data Processing (ADP) (Roseland , NJ)	ADP sent paperwork for a small Wisconsin company to a Cordova, TN coffee house. The paperwork contained names, birth dates, SSNs, addresses, salaries, and bank account and routing numbers	Unknown
Nov. 16, 2006	American Cancer Society (Louisville , KY, offices, HQ in Atlanta , GA) If you have tips, call (502) 574-5673	An unspecified number of laptop computers were stolen from the Louisville offices of the American Cancer Society. It is not clear what personal information was exposed, if any.	Unknown
Nov. 16, 2006	Carson City residents (Carson City, NV)	The Sheriff's Department reported that at least 50 residents had their credit card information stolen by employees of local businesses. The employees apparently sell the account information to international crime rings that produce counterfeit cards. The crime is called "skimming."	50
Nov. 15, 2006	Internal Revenue Service	According to document s obtained under the Freedom of Information Act, 478 laptops were either lost or	2,359

	(Washington, DC)	stolen from the IRS between 2002 and 2006. 112 of the computers held sensitive taxpayer information such as SSNs. **UPDATE** (04/05/07): A report by the Treasury Inspector General for Tax Administration noted that at least 490 IRS computers have been stolen or lost since 2003 in 387 security breach incidents that potentially jeopardized tax payers' personal information. **UPDATE** (04/17/07): The Inspector General's assessment of 20 buildings in 10 cities discovered four separate locations at which hackers could have easily gained access to IRS computers and taxpayer data using wireless technology.	
Nov. 13, 2006	Connors State College (Warner, OK) (918) 463-6267 perline@ connorsstate.edu	On Oct. 15, a laptop computer was discovered stolen from the college. (It has since been recovered by law enforcement). The computer contains Social Security numbers and other data for Connors students plus 22,500 high school graduates who qualify for the Oklahoma Higher Learning Access Program scholarships.	Considerably more than 22,500
Nov. 10, 2006	KSL Services, Inc. (Los Alamos, NM)	A disk containing the personal information of approximately 1,000 KSL employees is missing. KSL is a contractor for Los Alamos National Laboratory.	Approximately 1,000
Nov. 9, 2006	Four ARCO gas stations (Costa Mesa, CA) (Westminster, CA) (Torrance, CA)	From Sept. 29 to Oct. 9, thieves used card skimmers to steal bank account numbers and PIN codes from gas station customers and used the information to fabricate debit cards and make ATM withdrawals.	At least 440
Nov 7, 2006	City of Lubbock (Lubbock, TX)	Hackers broke into the city's web site and compromised the online job application database, which included Social Security numbers.	5,800
Nov. 3, 2006	University of Virginia (Charlottesville, VA)	Due to a computer programming error, Student Financial Services sent e-mail messages to students containing 632 other students' Social Security numbers.	632 students
Nov. 3, 2006	West Shore Bank (Ludington, MI)	Customers' debit cards and possibly credit cards were compromised from a security break last summer at a common MasterCard point-of-purchase provider.	About 1,000
Nov. 3, 2006	Wesco (Muskegon, MI)	Wesco gas stations experienced a breach in credit card transactions from July 25-Sept. 7 resulting in inaccurate charges to customer accounts.	Unknown
Nov. 3, 2006	Starbucks Corp. (Seattle, WA) 1-800-453-1048	Starbucks lost track of four laptop computers. Two held employee names, addresses, and Social Security numbers.	60,000 current and former U.S. employees and about 80 Canadian workers and contractors
Nov. 3, 2006	Several Joliet area motels (Joliet, IL)	Motel owners and employees allegedly stole and sold customers' credit card numbers.	Unknown
Nov. 2, 2006	Colorado Dept. of Human Services via Affiliated Computer Services (ACS) (Dallas, TX) For questions, call ACS at (800) 350-0399	On Oct. 14, a desktop computer was stolen from a state contractor who processes Colorado child support payments for the Dept. of Human Services. Computer also contained the state's Directory of New Hires. **UPDATE** (12/07/2006) When initially posted to this list, the number 1.4 million was **not** added to the total because we could not confirm if SSNs were exposed. The PRC was contacted by an affected individual today who confirmed that names, addresses, **SSNs** and dates of birth were exposed.	Up to 1.4 million
Nov. 2, 2006	Greater Media, Inc. (Philadelphia, PA)	A laptop computer containing the Social Security numbers of the radio broadcasting company's current and former employees was stolen from their Philadelphia offices.	Unknown
Nov. 2, 2006	McAlester Clinic and Veteran's Affairs Medical Center (Muskogee, OK)	Three disks containing billing information, patient names and Social Security numbers, were lost in the mail.	1,400 veterans
Nov. 2, 2006	Intermountain Health Care (Salt Lake City, UT)	A computer was purchased at a second-hand store, Deseret Industries, that contained the names, Social Security numbers, employment records, and other personal information about Intermountain Health Care	6,244

		employees employed there in 1999-2000.	
Nov. 2, 2006	Compulinx (White Plains, NY)	The CEO of Compulinx was arrested for fraudulently using employees' names, addresses, Social Security numbers and other personal information for credit purposes. (It is unclear whether customers' data was also used).	Up to 50 Compulinx employees
Nov. 2006	Home Finance Mortgage, Inc. (Cornelius, NC)	Company dumped files containing names, addresses, Social Security numbers, credit card numbers, and bank account numbers of people who had applied for mortgage loans. Home Finance and its owners have agreed to pay the State of NC $3,000 for their violations.	Unknown
Nov. 1, 2006	U.S. Army Cadet Command (Fort Monroe, VA) 1-866-423-4474 Email: mydata@ usaac.army.mil	A laptop computer was stolen that contained the names, addresses, telephone numbers, birthdates, Social Security numbers, parent names, and mother's maiden names of applicants for the Army's four-year ROTC college scholarship.	4,600 high school seniors
Oct. 31, 2006	Avaya (theft occurred in Maitland, FL, office of company, headquartered in Basking Ridge, NJ)	A laptop stolen from an Avaya employee on October 16 in Florida contained personally identifiable information, including names, addresses, W-2 tax form information and SSNs.	Unknown
Oct. 30, 2006	Georgia county clerk of courts' web sites	A Georgia TV station reported that SSNs could be found on some records posted on county clerk of court web sites, specifically for individuals with federal tax liens filed against them. At least one county clerk -- Cherokee County -- is now removing SSNs from the web site.	Unknown
Oct. 30, 2006	Nissan Motor Co., Ltd. (Tokyo, Japan)	The Japanese weekly magazine "The Weekly Asahi" reported that Nissan experienced the leak of a database containing customers' personal information sometime between May 2003 and February 2004. The data includes the customer name, gender, birth date, address, telephone number, vehicle model owned (including base and class), and license plate number.	5,379,909 customers (not included in total because data apparently does not contain financial account information or SSNs)
Oct. 27, 2006	Gymboree (San Francisco, CA)	A thief stole 3 laptop computers from Gymboree's corporate headquarters. They contained unencrypted human resources data (names and Social Security numbers) of thousands of workers.	up to 20,000 employees
Oct. 27, 2006	Hancock Askew & Co. (Savannah, GA)	On October 5, 2006, a laptop computer containing 401(k) information for employees of at least one company (Atlantic Plastics, Inc.) was stolen from accounting firm Hancock Askew.	Unknown
Oct. 27, 2006	Hertz Global Holdings, Inc. (Oklahoma City, OK) 1-888-222-8086	The names and Social Security numbers of Hertz employees dating back to 2002 were discovered on the home computer of a former employee.	Unknown
Oct. 26, 2006	Akron Children's Hospital (Akron, OH)	Overseas hackers broke into two computers at Children's Hospital. One contains private patient data (including Social Security numbers) and the other holds billing and banking information.	235,903
Oct. 26, 2006	Empire Equity Group (Charlotte, NC)	Mortgage files that included personal financial details about loan applicants were found in a dumpster. Empire Equity will pay $12,500 to the State of NC.	Unknown
Oct. 26, 2006	LimeWire (Denver, CO)	The Denver Police Dept. reports that LimeWire's file-sharing program was exploited to access personal and financial information from approximately 75 different individual and business account names from all over the country. The information, which included tax records, bank account information, online bill paying records and other material, appears to have been stolen directly from computers that were using LimeWire's filesharing software program.	75
Oct. 26, 2006	Hilb, Rogal & Hobbs (Plymouth Meeting, PA)	In September 2006, a laptop computer was stolen from the insurance brokerage firm. It contained client information including the names, birthdates, and drivers license numbers of Villanova University students and staff who drive university vehicles.	1,243 Villanova University students and staff

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Oct. 25, 2006	Transportation Security Administration (TSA) (Portland, OR)	A thumb drive is missing from the TSA command center at Portland International Airport and believed to contain the names, addresses, phone numbers and Social Security numbers of approximately 900 current and former employees.	900 current and former Oregon TSA employees
Oct. 25, 2006	Swedish Medical Center, Ballard Campus (Seattle, WA) (800) 840-6452	An employee stole the names, birthdates, and Social Security numbers from patients who were hospitalized or had day-surgeries from June 22 to Sept 21. She used 3 patients' information to open multiple credit accounts.	Up to 1,100 patients
Oct. 25, 2006	Tuscarawas County and Warren County (OH)	The Social Security numbers of some Tuscarawas and Warren County voters were available on the LexisNexis Internet database service. **UPDATE** (11/1/06): LexisNexis says it has now removed the SSNs.	Unknown
Oct. 24, 2006	Jacobs Neurological Institute (Buffalo, NY)	The laptop of a research doctor was stolen from her locked office at the Institute. It included records of patients and her research data.	Unknown
Oct. 23, 2006	Sisters of St. Francis Health Services via Advanced Receivables Strategy (ARS), a Perot Systems Company (Indianapolis, IN) (866) 714-7606	On July 28, 2006, a contractor working for Advanced Receivables Strategy, a medical billing records company, misplaced CDs containing the names and SSNs of 266,200 patients, employees, physicians, and boad members of St. Francis hospitals in Indiana and Illinois. Also affected were records of Greater Lafayette Health Services. The disks were inadvertently left in a laptop case that was returned to a store. The purchaser returned the disks. The records were not encrypted even though St. Francis and ARS policies require encryption.	260,000 patients and about 6,200 employees, board members and physicians for a total of 266,200
Oct. 23, 2006	Chicago Voter Database (Chicago, IL)	An official from the not-for-profit Illinois Ballot Integrity Project says his organization hacked into Chicago's voter database, compromising the names, SSNs and dates of birth of 1.35 million residents. The Chicago Election Board is reportedly looking into removing SSNs from the database. Election officials have patched the flaw that allowed the intrusion.	1.35 million Chicago residents
Oct. 21, 2006	Bowling Green Police Dept. (Bowling Green, OH)	The police dept. accidentally published a report on their website containing personal information on nearly 200 people the police had contact with on Oct. 21. Data included names, Social Security numbers, driver's license numbers, etc.	Approx. 200 victims or suspects
Oct. 20, 2006	Manhattan Veteran's Affairs Medical Center, New York Harbor Health Care System (New York, NY)	On Sept. 6, an unencrypted laptop computer containing veterans' names, Social Security numbers, and medical diagnosis, was stolen from the hopsital.	1,600 veterans who receive pulmonary care at the facility
Oct. 19, 2006	Allina Hospitals and Clinics (Minneapolis-St. Paul, MN)	A laptop stolen from a nurse's car on October 8 contains the names and SSNs of individuals in approximately 17,000 households participating in the Allina Hospitals and Clinics obstetric home-care program since June 2005.	Individuals in 17,000 households
Oct. 19, 2006	University of Minnesota/Spain	In June, a University of Minnesota art department laptop computer stolen from a faculty member while traveling in Spain holds personally identifiable information of 200 students.	200 students (not included in total)
Oct. 17, 2006	City of Visalia, Recreation Division (Visalia, CA)	Personally identifiable information of approximately 200 current and former Visalia Recreation Department employees was exposed when copies of city documents were found scattered on a city street.	200 current and former employees
Oct. 16, 2006	Germanton Elementary School (Germanton, NC)	A computer stolen from Germanton Elementary school holds students' SSNs. The data on the computer are encrypted.	Unknown
Oct. 16, 2006	VISA/FirstBank	FirstBank sent a letter to an unknown number of customers informing them their FirstTeller Visa Check Card numbers were compromised when someone accessed “a merchant card processor's transaction database.” The FirstBank letter said customers would receive new cards by October 27.	Unknown
Oct. 16, 2006	Dr, Charles Kay of Orchard Family Practice (Englewood, CO)	Sheriff's deputies evicting Dr. Charles Kay put files from his office in a nearby parking lot. In a news report, Dr. Kay said he had removed the patient files but not the business files.	Unknown

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

Oct. 15, 2006	Poulsbo Department of Licensing (Poulsbo, WA)	An unspecified “storage device” containing personally identifiable data of approximately 2,200 North Kitsap (WA) residents has been lost from the Poulsbo Department of Licensing. The data include names, addresses, photographs and driver's license numbers of individuals who conducted transactions at the Poulsbo branch in late September.	2,200
Oct. 14, 2006	T-Mobile USA Inc. (Bellvue, WA)	A laptop computer holding personally identifiable information of approximately 43,000 current and former T-Mobile employees disappeared from a T-Mobile employee's checked luggage. T-Mobile has reportedly sent letters to all those affected. The data are believed to include names, addresses, SSNs, dates of birth and compensation information.	43,000 current and former employees
Oct. 13, 2006	Ohio Ethics Committee (Columbus, OH)	Papers belonging to the Ohio Ethics Commission were found floating on the wind in an alley. The documents are related to state employees' finances and contained SSNs and financial statements. They were supposed to be in the possession of the state archives.	Unknown number of Ohio state employees
Oct. 13, 2006	Orchard Family Practice (Englewood, CO)	When a bankrupt Colorado doctor was evicted from his office, the landlord with help from the sheriff's dept.dumped everything from his office in the parking lot, including file cabinets containing personal information of his patients. Scavengers were seen carting off desks and file cabinets, some containing records. The exposed documents were thought to consist of business records containing names, SSNs, dates of birth, and addresses, but not medical information, which the doctor had previously removed.	Unknown
Oct. 12, 2006	U.S. Census Bureau	This spring, residents of Travis County, TX helped the Census Bureau test new equipment. When the test period ended, 15 devices were unaccounted for. The Census Bureau and the Commerce Department issued a press release saying the devices held names, addresses and birthdates, but not income or SSNs.	Unknown number of Travis Co., TX, residents
Oct. 12, 2006	Congressional Budget Office (Washington, D.C.)	Hackers broke into the Congressional Budget Office's mailing list and sent a phishing e-mail that appeared to come from the CBO.	Unknown number of e-mail addresses
Oct. 12, 2006	University of Texas at Arlington	Two computers stolen from a University of Texas faculty member's home hold the names, SSNs, grades, e-mail addresses and other information belonging to approximately 2,500 students enrolled in computer science and engineering classes between fall 2000 and fall 2006. The theft occurred on September 29 and was reported on October 2.	2,500 students
Oct. 11, 2006	Republican National Committee (Washington, D.C.)	The Republican National Committee (RNC) inadvertently emailed a list of donors' names, SSNs and races to a New York Sun reporter.	76 RNC donors
Oct. 10, 2006	Florida Labor Department	The names and SSNs of 4,624 Floridians were accessible on the Internet for approximately 18 days in September. The data were not accessible through Web sites, but an individual came across the information when Googling his own name. The agency has asked Google to remove the pages from its cache, and has notified all affected individuals by mail.	4,624 individuals who had registered with Florida 's Agency for Workforce Innovation
Oct. 6, 2006	Cleveland Air Route Traffic Control Center (Oberlin, OH)	A computer hard drive missing from the Cleveland Air Route Traffic Control Center in Oberlin (OH) contains the names and SSNs of at least 400 air traffic controllers.	At least 400
Oct. 6, 2006	Camp Pendleton Marine Corps base via Lincoln B.P. Management (Camp Pendleton near Oceanside, CA)	A laptop missing from Lincoln B.P. Management Inc. holds personally identifiable data about 2,400 Camp Pendleton residents.	2,400
Oct. 5, 2006	San Juan Capistrano Unified School District (CA)	Five computers stolen from the HQ of San Juan Capistrano Unified School District likely contain the names, SSNs and dates of birth of district employees enrolled in an insurance program.	Unknown
Oct. 9, 2006 (Letter mailed Oct. 5, 2006)	Troy Athens High School (Troy, MI) (For questions or comments, call (248) 823-4035)	A hard drive stolen from Troy Athens High School in August contained transcripts, test scores, addresses and SSNs of students from the graduating classes of 1994 to 2004. The school district and the superintendent have notified all affected alumni by regular mail.	4,400

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Oct. 4, 2006	Orange County Controller (FL)	A Florida woman discovered her marriage license was visible on the Orange County (FL) controller's Web site with no information blacked out, not even SSNs. She discovered the breach because someone had applied for a loan in her name. The Orange County Comptroller is reportedly paying a vendor $500,000 to black out all SSNs by January 2008.	Unknown
Oct. 3, 2006	Cumberland County, PA	Cumberland County (PA) officials removed salary board meeting minutes from their Web site because they contained the SSNs of 1,200 county employees. The information was included in minutes from meetings prior to 2000. The county no longer uses SSNs as unique identifiers for employees. Employees will be informed of the data breach in a note included with their paychecks.	1,200 employees of the county
Oct. 3, 2006	Willamette Educational Service District (Salem, OR)	Seven computers stolen from a Willamette Educational service District office were believed to contain personal information of 4,500 Oregon high school students. Backup tapes indicate the computers hold information about the students' school clubs but do not contain sensitive information.	4,500 Oregon high school students [not included in total because not thought to contain sensitive info. such as SSNs]
Oct. 3, 2006	Picatinny Arsenal (Rockaway Twp., NJ) (If you have tips, call (973) 989-0652)	28 computers are missing from the Picatinny Arsenal, a Department of Defense Weapons Research Center. The computers were reported lost or stolen over the last two years. None of the computers was encrypted. Officials state the computers did not contain classified information.	Unknown
Oct. 2, 2006	Port of Seattle (Seattle, WA) (888) 902-PORT	Six CDs missing from the ID Badging office at Seattle-Tacoma International Airport hold the personal information of 6,939 airport workers. The data include names, addresses, birth dates, SSNs and driver's license numbers, telephone numbers, employer information, and height/weight. The data on the disks were scanned from paper applications for airport badges. The port learned of the missing disks on September 18 and sent letters to the affected employees on Oct. 2.	6,939 current and former Seattle-Tac International Airport employees
Sept. 29, 2006	University of Iowa Dept of Psychology (Iowa City, IA)	A computer containing SSNs of 14,500 psychology department research study subjects was the object of an automated attack designed to store pirated video files for subsequent distribution.	14,500 individuals who had participated in a research study
Sept. 29, 2006	Kentucky Personnel Cabinet (Frankfort, KY)	State employees received letters from the Kentucky Personnel Cabinet with their SSNs visible through the envelope windows.	146,000
Sept. 28, 2006	North Carolina Dept. of Motor Vehicles (Louisville , NC) (888) 495-5568	A computer was stolen from a NC Dept. of Motor Vehicles office, reported Sept. 10. It contains names, addresses, driver's license numbers, SSNs, and in some cases immigration visa information of 16,000 people who have been issued licenses in the past 18 months. Most are residents of Franklin County.	16,000
Sept. 28, 2006	Illinois Dept. of Transportation (Springfield, IL)	Documents found by state auditors in recycling bins in a hallway contained IDOT employee names and SSNs.	40
Sept. 28, 2006	Stevens Hospital Emergency Room via dishonest employee of billing company Med Data (Edmonds, WA)	A manager for the hospital's billing company, Med Data, stole patients' credit card numbers. She gave them to her brother who bought $30,000 worth of clothes and gift cards over the Internet. The woman is scheduled for sentencing in Nov. and her brother's trial is expected Jan. 2007.	"about 30 patients"
Sept. 25, 2006	Movie Gallery (Gastonia, NC)	A large number of Movie Gallery's files and videos were found in a dumpster. The files contained personal information of people employed by Movie Gallery and people applying for jobs at the video store as well as people applying for movie rental membership. Movie Gallery has agreed to pay $50,000 to the State of NC.	Unknown
Sept. 25, 2006	General Electric (US Corporate HQ: Fairfield , CT)	An employee's laptop computer holding the names and Social Security numbers of approximately 50,000 current and former GE employees was stolen from a locked hotel room while he was traveling for business.	50,000 employees
Sept. 23, 2006	An illegal dumping site northwest of Quinlan, TX	Investigators found boxes of private medical records containing names and personal information of patients of a doctor who lives in Dallas and who has a Greenville, TX, practice. They had apparently been dumped there by a contractor who was hired to remodel his house. The contractor was indicted on a charge of illegal dumping.	Unknown

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Sept. 23, 2006	Erlanger Health System (Chattanooga, TN)	Records of hospital employees disappeared from a locked office on Sept. 15. They were stored on a USB "jump drive." Information was limited to names and SSNs. Those affected included anyone who went through job "status changes" from Nov. 2003 to Sept. 2006.	4,150 current and former employees
Sept. 22, 2006	Purdue University College of Science (West Lafayette, IN) (866) 307-8520 www.purdue.edu	A file in a desktop computer in the Chemistry Department may have been accessed illegitimately. The file contained names, SSNs, school, major, and e-mail addresses of people who were students in 2000.	2,482 students from the year 2000
Sept. 22, 2006	University of Colorado-Boulder, Leeds School of Business (Boulder, CO) (303) 492-8741	Two computers had been placed in storage during the school's move to temporary quarters in May. When they were to be retrieved Aug. 28, they were found missing. They had been used by 2 faculty members and included students' names, SSNs, and grades. **UPDATE** (9/25/06): One of the computers was found.	1,372 students and former students
Sept. 22, 2006	Several Indianapolis pharmacies (Indianapolis, IN)	Earlier this year a local TV reporter from WTHR found that "dozens" of pharmacies disposed of customer records in unsecured garbage bins. Now the Indiana Board of Pharmacy has launched an investigation of 30 pharmacies. Both the Board and the Attorney General say that the pharmacies violated state law.	Unknown
Sept. 21, 2006	Pima Co. Health Dept. (Tucson, AZ)	Vaccination records on 2,500 clients had been left in the trunk of a car that was stolen Sept. 12. The car and records have since been recovered. Records included names, dates of birth and ZIP codes, but no SSNs or addresses.	2,500 (not included in Total below)
Sept. 21, 2006	U.S. Dept. of Commerce and Census Bureau (Washington, DC)	The agency reported that 1,137 laptops have been lost or stolen since 2001. Of those, 672 were used by the Census Bureau, with 246 of those containing personal data. Secretary Gutierrez said the computers had "protections to prevent a breach of personal information."	Unknown
Sept. 20, 2006	City of Savannah, Georgia (912) 651-6565 savannahga.gov	Because of a "hole in the firewall,"a City server exposed personal information online for 7 months. Individuals identified by the Red Light Camera Enforcement Program are affected -- name, address, driver's license number, vehicle identification number, and SSNs of those individuals whose driver's license number is still the SSN.	8,800 individuals whose identities were captured by red-light cameras
Sept. 20, 2006	Berry College via consultant Financial Aid Services Inc. (Mount Berry, GA) (800) 961-4692 www.berry.edu	Student applications for need-based financial aid were misplaced by a consultant -- in both paper and digital form. Data included name, SSN, and reported family income for students and potential students for the 2005-06 academic year.	2,093 students and potential students (of those, 1,322 are currently enrolled)
Sept. 19, 2006	Life Is Good (Hudson, NH)	Hackers accessed the retailer's database containing customer's credit card numbers. The company said no other personal information was in the database.	9,250 customers' credit card numbers
Sept. 18, 2006	Howard, Rice, Nemerovski, Canady, Falk & Rabkin law firm (San Francisco, CA) via its auditor Morris, Davis & Chan (Oakland, CA)	A laptop was stolen from the trunk of the car of the law firm's auditor, containing confidential employee pension plan information -- names, SSNs, remaining balances, 401(k) and profit-sharing information.	500 current and former employees
Sept. 18, 2006	DePaul Medical Center, Radiation Therapy Dept. (Norfolk, VA) (757) 889-5945	Two computers were stolen, one on August 28 and the other Sept. 11. Personal data included names, date of birth, treatment information, and some SSNs.	"More than 100 patients"
Sept. 17, 2006	Direct Loans, part of William D. Ford Federal Direct Loan Program within U.S. Dept. of Education and Federal Student Aid via its IT contractor ACS	A security breach exposed private information of student loan borrowers from Aug. 20-22 during a computer software upgrade. Users of the Direct Loans Web site were able to view information other than their own if they used certain options. SSNs were among the data elements exposed online.	21,000 accounts
Sept. 16, 2006	Michigan Dept. of Community Health (Detroit, MI)	Residents who participated in a scientific study were notified that a flash drive was discovered missing as of Aug. 4, and likely stolen, from an MDCH office.The portable memory device contained names,	4,000 Michigan residents

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

		addresses, phone numbers, dates of birth, and SSNs of participants. The study tracked the long-term exposure to flame retardents ingested by residents in beef and milk.	
Sept. 16, 2006	Beaumont Hospital (Royal Oak, MI)	The hospital mistakenly mailed medical reports on 3 patients to a retired dentist in Texas. Reports included name, test results, date of birth and patient ID numbers. The hospital admitted to both human and computer error. A new computer system mixed similar names, and staff did not catch it.	3 patients
Sept. 15, 2006	Mercy Medical Center (Merced, CA)	A memory stick containing patient information was found July 18 by a local citizen on the ground at the County Fairgrounds near the hospital's information booth. It was returned to the hospital 4 weeks later. Data included names, SSNs, birthdates, and medical records.	295 patients
Sept. 15, 2006	Whistle Junction restaurant (Orlando, FL)	Personnel files of employees of the now-closed restaurant were found in a nearby Dumpster. Papers included names and SSNs of former employees,	Unknown
Sept. 14, 2006	Nikon Inc. and Nikon World Magazine (Melville, NY)	Workers at a Montgomery, AL, camera store discovered that subscription information for the magazine Nikon World was exposed on the Web for at least 9 hours. Data included subscribers' names, addresses and credit card numbers.	3,235 magazine subscribers
Sept. 14, 2006	Illinois Dept. of Corrections (Springfield, IL)	A document containing employees' personal information was found outside the agency's premises "where it should not have been." It has since been retrieved. Information included employees' names, SSNs, and salaries.	Unknown
Sept. 13, 2006	American Family Insurance (Madison, WI)	The office of an insurance agent was broken into and robbed last July. Among the items stolen was a laptop with customers' names, SSNs, and driver's license numbers.	2,089 customers
Sept. 11, 2006	Telesource via Vekstar (Indianapolis, IN)	Employees discovered their personnel files in a Dumpster after the company had been bought out by another company Vekstar. The files were discarded when the office was being cleaned out and shut down. Files contained SSNs, dates of birth and photocopies of SSN cards and driver's licenses.	Unknown
Sept. 9, 2006	Cleveland Clinic (Naples, FL) (866) 907-0675	A clinic employee stole personal information from electronic files and sold it to her cousin, owner of Advanced Medical Claims, who used it to file fraudulent Medicare claims totaling more than $2.8 million. Information included names, SSNs, birthdates, addresses and other details. Both individuals were indicted.	1,100 patients
Sept. 8, 2006	Linden Lab (San Francisco, CA) www.secondlife.com	On Sept. 6, Linden Lab discovered that a hacker accessed its Second Life database through web servers. The affected data included unencrypted account names, real life names, and contact information, plus encrypted account passwords and payment information. Second Life is a 3-D virtual world.	Unknown
Sept. 8, 2006	University of Minnesota (Minneapolis, MN)	On August 14-15 eve, two computers were stolen from the desk of an Institute of Technology employee, containing information on students who were freshmen from 1992-2006 -- including names, birthdates, addresses, phone numbers, high schools attended, student ID numbers, grades, test scores, and, academic probation. SSNs of 603 students were also exposed.	13,084 students including SSNs of 603 students
Sept. 8, 2006	Berks Co. Sheriff's Office via contractor Canon Technology Solutions (Reading, PA)	A confidential list of some of the County's 25,000 gun permit holders was exposed on the Web by the contractor that is developing a Web-based computer records program for the Sheriff's Office. Personal information included names, addresses and SSNs. **UPDATE** (10/6/06): The Berks County solicitor's office says the entire list of more than 25,000 gun permit holders was exposed.	25,000 gun permit holders exposed, although initially the number was unknown
Sept. 7, 2006	Florida National Guard (Bradenton, FL)	A laptop computer was stolen from a soldier's vehicle contained training and administrative records, including Social Security numbers of up to 100 Florida National Guard soldiers.	100
Sept. 7, 2006	Circuit City and Chase Card Services, a division of JP Morgan Chase & Co. (Wilmington, DE)	Chase Card Services mistakenly discarded 5 computer data tapes in July containing Circuit City cardholders' personal information.	2.6 million past and current Circuit City credit cardholders
Sept. 5, 2006	Transportation Security Administration (TSA) via Accenture	In late August 2006, Accenture, a contractor for TSA mailed documents containing former employees' SSN,, date of birth, and salary information to the wrong addresses due to an administrative error.	1,195 former TSA employees

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	(Washington, DC)		
Sept. 2, 2006	Iowa Student Loan (W. Des Moines)	Compact disk containing personal information, including SSNs, was lost when shipped by private courier.	165,000
Sept. 2, 2006	Lloyd's of London (Port St. Lucie, FL)	A thief reprogrammed more than 150 Lloyd's of London credit card numbers onto phone cards and used them to withdraw money from an ATM in Port St. Lucie, FL (stealing more than $20,000 over 3 days). Key personal and financial information had been skimmed from the magnetic strip on the victims' cards.	Unknown
Sept. 1, 2006	Wells Fargo via unnamed auditor (San Francisco, CA)	In a letter dated Aug. 28, the company notified its employees that a laptop and data disk were stolen from the locked trunk of an unnamed auditor, hired to audit the employees' health plan. Data included names, SSNs, and information about drug claim cost and dates from 2005, but no prescription information said the company.	Unknown
Sept. 1, 2006	Virginia Commonwealth University (Richmond, VA) www.ts.vcu.edu	Personal information of freshmen and graduate engineering students from 1998 through 2005 was exposed on the Internet for 8 months (Jan. - Aug.) due to human error. It was discovered by a student who used a search engine to find her name. The data included SSNs and e-mail addresses.	2,100 current and former students
Sept. 1, 2006	City of Chicago via contractor Nationwide Retirement Solutions, Inc. (Chicago, IL) (800) 638-1485 www.chicagofop.org	A laptop was stolen from the home of contractor's employee last April 2005. It was reported to the city July 2006 more than a year later. Data included names, addresses, phone numbers, birthdates and SSNs for those in the city's deferred compensation plan.	"Up to 38,443 city employees and retirees"
Sept. 1, 2006 (Extact Date Unkown)	Adams State College (Alamosa, CO)	A laptop computer stolen from a locked closet at Adams State College contained personally identifiable data belonging to 184 high school students who participated in the college's Upward Bound program over the last four years. The theft occurred on August 14, but it was not until late September that staff realized the computer held students' data.	184 Upward Bound students
Aug. 31, 2006	Labcorp (Monroe, NJ) (800) 788-9091 x3925	During a break-in June 4 or 5, a computer was stolen that contained names and SSNs, but according to the company did not have birth dates or lab test results.	Unknown
Aug. 31, 2006	Diebold, Inc. (Canton, OH)	An employee's laptop was stolen containing employee information, including name, SSN, and if applicable, corporate credit card number.	Unknown
Aug. 29, 2006	Valley Baptist Medical Center (Harlingen, TX) (877) 840-5999	A programming error on the hospital's web site exposed names, birth dates, and SSNs of healthcare workers in late August. The error was fixed but it is not known how long the personal information was compromised. The affected individuals are workers from outside the hospital who provide services and bill the hospital via an online form.	Unknown
Aug. 29, 2006	AT&T via vendor that operates an order processing computer (San Francisco, CA)	Computer hackers accessed credit card account data and other personal information of customers who purchased DSL equipment from AT&T's online store. The company is notifying "fewer than 19,000" customers." **UPDATE** (9/1/06). The breach was followed by a bogus phishing e-mail to those customers that attempted to trick them into revealing more info such as SSN and birthdate -- essential for crime of identity theft.	"Fewer than 19,000" customers
Aug. 29, 2006	Compass Health (Everett, WA) (800) 508-0059	Compass Health notified some of its clients that a laptop containing personal information, including SSNs, was stolen June 28. The agency serves people who suffer from mental illness.	"A limited number of people"
Aug. 27, 2006	New Mexico Administrative Office of the Courts (Santa Fe, NM)	For 8 days in late May, an unsecured document was exposed on the agency's FTP site on the state's computer server. It contained names, birth dates, SSNs, home addresses and other personal information of judicial branch employees. The FTP site was shut down June 2 and has since be redesigned.	1,500 employees
Aug. 26, 2006	PortTix (Portland, ME)	Credit card information for about 2,000 people who ordered tickets online through PortTix was accessed by someone who hacked into the Web site. PortTix is Merrill Auditorium's ticketing agency. The Web site was secured as of Aug. 24.	2,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Aug. 26, 2006	University of South Carolina (Columbia, SC)	A security audit this summer found that a computer server was hacked in Sept. 2005. A database could have been accessed with names, SSNs, and birthdates of current and former students.	6,000 current and former students
Aug. 25, 2006	Dominion Resources (Richmond, VA)	Two laptops containing employee information were stolen earlier in August. It was not clear what type of data were included. No customer records were on the computers. Dominion operates a gas and electric energy distribution company.	Unknown
Aug. 25, 2006	U.S. Dept. of Transportation, Federal Motor Carrier Safety Administration (Baltimore, MD) (800) 832-5660	A laptop that "might contain" personal information of people with commercial driver's licenses was stolen Aug. 22. FMCSA said the data might include names, dates of birth, and commercial driver's license numbers of 193 individuals from 40 trucking companies.	193 (not added to total)
Aug. 25, 2006	Sovereign Bank (New Bedford, MA)	Personal data may have been compromised when 3 managers' laptops were stolen from 2 separate locations in early August. Customers were notified Aug. 21. Sovereign serves New England and the Mid-Atlantic. The bank said the data included unspecified customer information, but not account data.	"thousands of customers"
Aug. 23, 2006	U.S. Dept. of Education, Direct Loan Servicing Online (Atlanta, GA) www.dlssonline.com and dlservicer.ed.gov	A faulty Web site software upgrade resulted in personal information of 21,000 student loan holders being exposed on the Department's loan Web site. Information included names, birthdates, SSNs, addresses, phone numbers, and in some cases, account information. Affiliated Computer Services Inc. is the contractor responsible for the breach. The breach did not include those whose loans are managed through private companies.	21,000
Aug. 22, 2006	AFLAC American Family Life Assurance Co. (Greenville, SC) (888) 794-2352	A laptop containing customers' personal information was stolen from an agent's car. It contained names, addresses, SSNs, and birth dates of 612 policyholders. They were notified Aug. 11.	612 policyholders
Aug. 22, 2006	Beaverton School District (Beaverton, OR)	Time slips revealing personal information were missing and presumed stolen following a July 24 break-in at a storage shed on the administration office's property. The time slips included names and SSNs but not addresses.	1,600 employees
Aug. 22, 2006	Beaumont Hospital (Troy, MI)	A vehicle of a home health care nurse was stolen from outside a senior center Aug. 5. Although it was recovered nearby, a laptop left in the rear of the car was not recovered. It contained names, addresses, SSNs, and insurance information of home health care patients. **UPDATE** (8/23/06). The laptop was returned Aug. 23 by a woman who said she found it in her yard.	28,400 home care patients
Aug. 21, 2006	U.S. Dept. of Education via contractor, DTI Associates (Washington, DC)	Two laptops were stolen from DTI's office in downtown DC containing personal information on 43 grant reviewers for the Teacher Incentive Fund. DTI could not rule out that the data included SSNs.	43
Aug. 18, 2006	Calif. Dept. of Mental Health (916) 654-2309	Computer tape with employees' names, addresses, and SSNs has been reported missing. Employees were notified Aug. 17 by e-mail.	9,468 employees
Aug. 17, 2006	Williams-Sonoma (San Francisco, CA)	On July 10, a laptop was stolen from the Los Angeles home of a Deloitte & Touche employee who was conducting an audit for W-S. Computer contained employees' payroll information and SSNs.	1,200 current and former employees
Aug. 17, 2006	HCA, Inc. Hospital Corp. of America (Nashville, TN) (800) 354-1036 hcahealthcare.com	10 computers containing Medicare and Medicaid billing information and records of employees and physicians from 1996-2006 were stolen from one of the company's regional offices. Some patient names and SSNs were exposed, but details are vague. Records for patients in hospitals in the following states were affected: CO, KS, LA, MS, OK, OR, TS, WA.	"thousands of files"
Aug. 16, 2006	Chevron (San Ramon, CA)	Chevron informed its U.S. workers Aug. 14 that a laptop was stolen from "an employee of an independent public accounting firm" who was auditing its benefits plans. The theft apparently occurred Aug. 5. Files contained SSNs and sensitive information related to health and disability plans.	Total employees affected is unclear. Nearly half of its 59,000 workers are from North America.
Aug. 15, 2006	University of Kentucky	The names and SSNs of 630 students were posted on the University's financial aid web site between	630

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

		Friday and Monday, Aug. 11-14.	
Aug. 15, 2006	University of Kentucky	About 80 geography students were notified Aug. 14 that their SSNs were inadvertently listed on an e-mail communication they all received telling them who their academic advisor would be for the coming year.	80
Aug. 15, 2006	U.S. Dept. of Transportation (Orlando, FL)	On April 24, a DOT employee's laptop computer was stolen from an Orlando hotel conference room. It contained several unencrypted case files. Investigators are determining if it contained sensitive personal information.	Unknown
Aug. 11, 2006	Madrona Medical Group (Bellingham, WA)	On Dec. 17, 2005, a former employee accessed and downloaded patient files onto his laptop computer. Files included name, address, SSN, and date of birth. The former employee has since been arrested.	At least 6,000 patients
Aug. 9, 2006	U.S. Dept. of Transportation (800) 424-9071 hotline@ oig.dot.gov	The DOT's Office of the Inspector General reported a special agent's laptop was stolen on July 27 from a government-owned vehicle in Miami, FL, parked in a restaurant parking lot. It contained names, addresses, SSNs, and dates of birth for 80,670 persons issued commercial drivers licenses in Miami-Dade County; 42,800 persons in FL with FAA pilot certificates; and 9,000 persons with FL driver's licenses. **UPDATE** (11/21/06): A suspect was arrested in the same parking lot where the theft occurred, but the laptop has not been recovered. Investigators found a theft ring operating in the vicinity of the restaurant parking lot.	132,470
Aug. 8, 2006	Virginia Bureau of Insurance (804) 726-2630	The Bureau has advised insurance agents in the state that their SSN may have been exposed on its web site from June 13 through July 31, 2006, due to a programming error. The SSNs were not shown on any web page, but could have been found by savvy computer users using the source code tool of a web browser.	Unknown
Aug. 8, 2006	Linens 'n Things (Sterling, VA)	A folder holding about 90 receipts was missing from the store. Receipts included full credit or debit account number and name of the card holder.	90
Aug. 7, 2006	U.S. Dept. of Veteran's Affairs through its contractor Unisys Corp. (Reston, VA)	Computer at contractor's office was reported missing Aug. 3, containing billing records with names, addresses, SSNs, and dates of birth of veterans at 2 Pennsylvania locations. **UPDATE** (9/15/06): Law enforcement recovered the computer and arrested an individual who had worked for a company that provides temporary labor to Unisys.	5,000 Philadelphia patients, 11,000 Pittsburgh patients, 2,000 deceased patients, plus possibly 20,000 more (18,000 is included in total below)
Aug. 6, 2006	American Online (AOL) (nationwide)	In late July AOL posted on a public web site data on 20 million web queries from 650,000 users. Some search records exposed SSNs, credit card numbers, or other pieces of sensitive information. **UPDATE** (9/26/06): Three individuals whose data were exposed have filed a lawsuit against AOL.	Unknown how many records contain high-risk personal information
Aug. 4, 2006	Toyota plant (San Antonio, TX)	Laptop belonging to contractor and containing personal information of job applicants and employees was stolen. Data included names and SSNs.	1,500
Aug. 4, 2006	PSA HealthCare (Norcross, GA) (866) 752-5259	A company laptop was stolen from an employee's vehicle in a public parking lot July 15. It contained names, addresses, SSNs, and medical diagnostic and treatment information used in reimbursement claims.	51,000 current and former patients
Aug. 1, 2006	U.S. Bank (Covington, KT)	A bank employee's briefcase was stolen from the employee's car with documents containing names, phone numbers, and SSNs of customers.	"very small" number
Aug. 1, 2006	Wichita State University (Wichita, KS)	WSU learned on June 29 that someone gained unauthorized access into 3 computers in its College of Fine Arts box office, containing credit card information for about 2,000 patrons.	2,000
Aug. 1, 2006	Wichita State University (Wichita, KS)	An intrusion into a WSU psychology department's server was discovered July 16. It contained information on about 40 applicants to the doctoral program.	40 (not included in total below because it is not known if SSNs were included in breached data)

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Aug. 1, 2006	Dollar Tree (Carmichael and Modesto, CA, as well as Ashland, OR, and perhaps other locations)	Customers of the discount store have reported money stolen from their bank accounts due to unauthorized ATM withdrawals. Data may have been intercepted by a thief's use of a wireless laptop computer with the thief then creating counterfeit ATM cards and using them to withdraw money. **UPDATE** (10/5/06): Parkev Krmoian was indicted by a federal grand jury for allegedly using phony ATM cards made from gift cards. The case is tied to the Dollar Tree customer bank account thefts.	Total number unknown
Aug. 1, 2006	Ron Tonkin Nissan (Portland, OR) Questions? Call: (503) 251-3349	Several months ago the car dealership experienced a security breach affecting the personal information of those who bought cars or applied for credit between 2001 and March 2006.	Up to 16,000 affected
Aug. 1, 2006 (Exact Date Unkown)	CoreLogic for ComUnity Lending (Sacramento, CA) (877) 510-3700 identityprotection@ corelogic.com	In early August, CoreLogic notified customers of ComUnity Lending that a computer with customers' data was stolen from its office. Data included names, SSNS, and property addresses related to an existing or anticipated mortgage loan.	Unknown
July 29, 2006	Sentry Insurance (Stevens Point, WI)	Personal information including SSNs on worker's compensation claimants was stolen, some of which was later sold on the Internet. No medical records were included. The thief was a lead programmer-consultant who had access to claimants' data. The consultant was arrested and faces felony charges.	Information on 72 claimants was sold on the Internet. Data on an additional 112,198 claimants was also stolen with no evidence of being sold online. Total affected is 112,270
July 28, 2006	Matrix Bancorp Inc. (Denver, CO) (877-250-7742)	Two laptop computers were stolen during daytime while staffers were away from their desks. One computer contained customers' account information. The bank says data is encrypted and password protected.	Unknown
July 28, 2006	Riverside, Calif., city employees	The SSNs and financial information regarding 401(k) accounts was accidentally e-mailed to 2,300 city employees due to a computer operator's error. The data was intended for the city payroll dept.	"nearly 2,000 employees"
July 27, 2006	Kaiser Permanente Northern Calif. Office (Oakland, CA) (866) 453-3934	A laptop was stolen containing names, phone numbers, and the Kaiser number for each HMO member. The data file did not include SSNs. The data was being used to market Hearing Aid Services to Health Plan members.	160,000 records. Because the data file did not include SSNs, this number is not added to the total below.
July 27, 2006	Los Angeles County (Los Angeles, CA)	In May, a laptop was stolen from the home of a community and senior services employee. It contained information on LA County employees.	Unknown
July 27, 2006	Los Angeles Co., Community Development Commission (CDC) (Monterey Park, CA)	Earlier in July, a computer hacker located in Germany gained access to the CDC's computer system, containing personal information on 4,800 public housing residents.	4,800 records. Because it is not clear if SSNs were included, this number is not added to the total below.
July 27, 2006	Los Angeles County, Adult Protective Services (Burbank, CA)	Last weekend 11 laptops were stolen from the Burbank office. It is not clear what type of personal information was included.	Unknown
July 26, 2006	U.S. Navy recruitment offices (Trenton, NJ, and Jersey City, NJ)	Two laptop computers with information on Navy recruiters and applicants were stolen in June and July. Also included was information from selective service and school lists. About 4,000 records contained SSNs. Files were password protected.	31,000 records were stolen, with about 4,000 containing SSNs. The latter number is included in the total below.
July 26, 2006	West Virginia Div. of Rehabilitation Services (Beckley, WV)	A laptop was stolen July 24 containing clients' names, addresses, SSNs, and phone numbers. Data was password protected.	Unknown

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

July 25, 2006	Armstrong World Industries (Lancaster Co., PA)	A laptop containing personal information of current and former employers was stolen. The computer was in the possession of the company's auditor, Deloitte & Touche. Data included names, home addresses, phone numbers, SSNs, employee ID numbers, salary data, and bank account numbers of employees who have their checks directly deposited.	12,000
July 25, 2006	Belhaven College (Jackson, MS)	An employee carrying laptop was robbed at gunpoint on July 19 while walking to his car. Computer contained names and SSNs of college employees.	300 employees
July 25, 2006	Georgetown University Hospital (Washington, DC)	Patient data was exposed online via the computers of an e-prescription provider, InstantDx. Data included names, addresses, SSNs, and dates of birth, but not medical or prescription data. GUH suspended the trial program with InstantDX.	"between 5,600 and 23,000 patients were affected" (23,000 added to total below)
July 25, 2006	Old Mutual Capital Inc., subsidiary of United Kingdom-based financial services firm Old Mutual PLC	Laptop was stolen sometime in May containing personal information of U.S. clients, including names, addresses, account numbers and some SSNs.	6,500 fund shareholders
July 25, 2006	Cablevision Systems Corp. (lost when shipped to Dallas-based ACS)	A tape en route to the company's 401(k) plan record-keeper ACS was lost when shipped by FedEx to Dallas, TX. No customer data was on the tape.	13,700 current and former employees
July 24, 2006	New York City Dept. of Homeless Services	The personal information of 8,400 homeless persons, including SSNs, was leaked in an e-mail attachment July 21, when accidentally sent to homeless advocates and city officials.	8,400
July 18, 2006	Nelnet Inc. (Lincoln, NE) (800) 552-7925	Computer tape containing personal information of student loan customers and parents, mostly from Colorado, was lost when shipped via UPS. The loans were previously serviced by College Access Network	188,000
July 18, 2006	CS Stars, subsidiary of insurance company Marsh Inc. (Chicago, IL)	On May 9, CS Stars lost track of a personal computer containing records of more than a half million New Yorkers who made claims to a special workers' comp fund. The lost data includes SSNs and date of birth but apparently no medical information. **UPDATE** (7/26/06): Computer was recovered. **UPDATE** (04/26/07): The New York Attorney General's office found that CS Stars violated the state's security breach law. CS Stars must pay the Attorney General's office $60,000 for investigation costs. It was determined that the computer had been stolen by an employee of a cleaning contractor, the missing computer was located and recovered, and that the data on the missing computer had not been improperly accessed.	540,000
July 18, 2006	U.S. Dept. of Agriculture (Wellington, KS)	Laptop computer and printout containing names, addresses and SSNs of 350 employees was stolen from an employee's car and later recovered.	350
July 17, 2006	Vassar Brothers Medical Center (Poughkeepsie, NY) (845) 483-6990	Laptop was stolen from the emergency department between June 23-26. It contained information on patients dating back to 2000, including SSNs and dates of birth. **UPDATE** (10/5/06) Private investigators determined the laptop did not contain personally identifiable patient information.	[257,800 patients were initially notified, but an analysis by Kroll later determined that the laptop contained no personal information. This number is not included in the total below.]
July 16, 2006	Mississippi Secretary of State (Jackson, MS)	The state agency's web site listed 2 million+ Uniform Commercial Code (UCC) filings in which thousands of individuals' SSNs were exposed.	Among the 2 million postings are "thousands" containings SSNs (not included in total)
July 14, 2006	Northwestern Univ. (Evanston, IL) (888-209-0097)	Files containing names and some personal information including SSNs were on 9 desktop computers that had been accessed by unauthorized persons outside the University. The computers were in the Office of Admissions and Financial Aid Office.	"As many as 17,000 individuals' records" exposed
July 14, 2006	University of Iowa	Laptop computer containing personal information of current and former MBA students was stolen. Data	280

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

	(Davenport, IA)	files included SSNs and some contact info.	
July 14, 2006 (Date of letter sent to students. Date of news story is 8/1/06)	California Polytechnic State University (Cal Poly) (San Luis Obispo, CA) (Call (805) 756-2226 or (805) 756-2171)	Laptop computer was stolen from the home of a physics department professor July 3. It included names and SSNs of physics and astronomy students from 1994-2004.	3,020 students
July 14, 2006	Treasurer's computer in Circuit Court Clerk's office (Hampton, VA)	Public computer in city government building containing taxpayer information was found to display SSNs of many residents -- those who paid personal property and real estate taxes. It was shut down and confiscated by the police on July 12th. **UPDATE:** (7/27/2006) Investigation concluded that the data was exposed due to software problem.	"Over 100,000 records" (The number containing SSNs is not known yet and not included in total below.)
July 13, 2006	Moraine Park Technical College (Beaver Dam, Fond du Lac, & West Bend, WI)	Computer disk (CD) with personal information of 1,500 students was reported missing. Information includes names, addresses, phone numbers & SSNs of apprenticeship students back to 1993.	1,500
July 7, 2006	University of Tennessee (866) 748-1680	Hacker broke into UT computer containing names, addresses and SSNs of about 36,000 past and current employees. Intruder apparently used computer from Aug. '05 to May '06 to store and transmit movies.	36,000
July 7, 2006	Nat'l Association of Securities Dealers (NASD) (Boca Raton, FL)	Ten laptops were stolen on Feb. 25 '06 from NASD investigators. They included SSNs of securities dealers who were the subject of investigations involving possible misconduct. Inactive account numbers of about 1,000 consumers were also contained on laptops.	73
July 7, 2006	Naval Safety Center	SSNs and other personal information of naval and Marine Corps aviators and air crew, both active and reserve, were exposed on Center web site and on 1,100 computer discs mailed to naval commands.	"more than 100,000"
July 7, 2006	Montana Public Health and Human Services Dept. (Helena, MT)	A state government computer was stolen from the office of a drug dependency program. during a 4th of July break-in. It was not known if sensitive information such as SSNs was compromised.	Unknown
July 7, 2006	City of Hattiesburg (Hattiesburg, MS)	Video surveillance cameras caught 2 intruders stealing hard drives from 18 computers June 23. Data files contained names, addresses, and SSNs of current and former city employees and registered voters as well as bank account information for employees paid through direct deposit and water system customers who paid bills electronically.	"thousands of city workers and contractors"
July 6, 2006	Automated Data Processing (ADP) (Roseland, NJ)	Payroll service company ADP gave scam-artist names, addresses, and number of shares held of investors, although apparently not SSNs or account numbers. The leak occurred from Nov. '05 to Feb. '06 and involved individual investors with 60 companies including Fidelity, UBS, Morgan Stanley , Bear Stearns, Citigroup, Merrill Lynch.	"Hundreds of thousands" [not included in total]
July 5, 2006	Bisys Group Inc. (Roseland, NJ)	Personal details about 61,000 hedge fund investors were lost when an employee's truck carrying backup tapes was stolen. The data included SSNs of 35,000 individuals. The tapes were being moved from one Bisys facility to another on June 8 when the theft occurred.	61,000
July 1, 2006	American Red Cross, Farmers Branch (Dallas, TX)	Sometime in May, 3 laptops were stolen, one of them containing encrypted personal information including names, SSNs, dates of birth, and medical information of all regional donors. They also report losing a laptop with encrypted donor information in June 2005.	Unknown
June 30, 2006	Nat'l Institutes of Health Federal Credit Union (Rockville, MD)	NIHFCU is investigating with law enforcement the identity theft of some of its 41,000 members. No details given on type of information stolen, or how it was stolen.	"Very few" of 41,000 members affected [not included in total]
June 29, 2006	AllState Insurance Huntsville branch (Huntsville, AL)	Over Memorial Day weekend, a computer containing personal data including images of insurance policies, correspondence and Social Security numbers was stolen.	2,700
June 29, 2006	Nebraska Treasurer's Office (Lincoln, NE)	A hacker broke into a child-support computer system and may have obtained names, Social Security numbers and other information such as tax identification numbers for 9,000 businesses.	309,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

June 29, 2006	Minnesota Dept. of Revenue (St. Paul, MN)	On May 16, a package containing a data tape used to back up the regional office's computers went missing during delivery. The tape contained personal information including individuals' names, addresses, and Social Security numbers. **UPDATE** (7/20/06)**:** The package was reported delivered 2 months later, but apparently had been temporarily lost by the U.S. Postal Service.	50,400
June 28, 2006	AAAAA Rent-A-Space (Colma, CA)	Customer's account information including name, address, credit card, and Social Security number was easily accessible due to a security gap in its online payment system.	13,000
June 27, 2006	Gov't Accountability Office (GAO) (Washington, D.C.)	Data from audit reports on Defense Department travel vouchers from the 1970s were inadvertently posted online and included some service members' names, Social Security numbers and addresses. The agency has subsequently removed the information.	"Fewer than 1,000" [1,000 used in total]
June 23, 2006	San Francisco State Univ. (San Francisco, CA)	a faculty member's laptop was stolen from a car on June 1 that contained personal information of former and current students including Social Security numbers, and names and ins some instance, phone numbers and grade point averages.	3,000
June 23, 2006	U.S. Navy (Washington, D.C.)	Navy personnel were notified on June 22 that a civilian web site contained files with personal information of Navy members and dependents including names, birth dates and Social Security numbers.	30,000
June 23, 2006	CA Dept. of Health Services (CDHS) (Sacramento, CA)	On June 12, a box of Medi-Cal forms from December 2005 were found in the cubicle of a CDHS employee. The claim forms contained the names, addresses, Social Security numbers and prescriptions for beneficiaries or their family members.	323
June 23, 2006	Catawba County Schools (Newton, NC)	On June 22, it was discovered that a web site posted names, Social Security numbers, and test scores of students who had taken a keyboarding and computer applications placement test during the 2001-02 school year. **UPDATE:** The web site containing the data has been removed.	619
June 23, 2006	King County Records, Elections, and Licensing Services Division (Seattle, WA)	Social Security numbers for potentially thousands of current and former county residents may be exposed on the agency's web site. Residents can request that the image of any document that contains a Social Security number, Mother's Maiden Name or Drivers License be removed. Officials state that they are unable to alter original public documents and cannot choose to not record documents presented for recording.	Unknown
June 22, 2006	Federal Trade Commission (FTC) (Washington, D.C.)	Two laptop computers containing personal and financial data were stolen from an employee's vehicle. The data included names, addresses, Social Security numbers, dates of birth, and in some instances, financial account numbers gathered in law enforcement investigations.	110
June 21, 2006	U.S. Dept. of Agriculture (USDA) (Washington, D.C.)	During the first week in June, a hacker broke into the Department's computer system and may have obtained names, Social Security numbers and photos of current and former employees and contractors.	26,000
June 21, 2006	Cape Fear Valley Health System (Fayetteville, NC)	Portable computer containing personal information of more than 24,000 people was stolen from ambulance of Cumberland Co. Emergency Medical Services on June 8th. It contained information on people treated by the EMS, including names, addresses, and birthdates, plus SSNs of 84% of those listed.	24,350
June 21, 2006 (Date of letter sent to doctors. Date of news story is July 28, 2006)	Lancaster General Hospital (Lancaster, PA)	A desktop computer with personal information of hundreds of doctors was stolen from a locked office June 10. The unencrypted data included names, practice addresses, and SSNS of physicians on medical and dental staff.	"Hundreds of local physicians" (not included in total below)
June 20, 2006	Equifax (Atlanta, GA)	On May 29, a company laptop containing employee names and partial and full Social Security numbers was stolen from an employee.	2,500
June 20, 2006	Univ. of Alabama (Birmingham, AL)	In February a computer was stolen from a locked office of the kidney transplant program at the University of Alabama at Birmingham that contained confidential information of donors, organ recipients and potential recipients including names, Social Security numbers and medical information.	9,800

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

June 17, 2006	ING (Washington, D.C.)	Laptop stolen from employee's home containing retirement plan information including Social Security numbers of D.C. city employees.	13,000
June 17, 2006	Automatic Data Processing (ADP) (Roseland, NJ)	Personal and payroll information of workers were intended to be faxed between ADP offices and were mistakenly sent to a third party.	80
June 17, 2006	CA Dept. of Health Services (CDHS) (Sacramento, CA)	CDHS documents were inappropriately emptied from an employee's cubicle on June 5 and 9 rather than shredded. The documents contained state employees and other individuals applying for employment with the state including names, addresses, Social Security numbers and home and work telephone numbers. They were mostly expired state employment certification lists, but also included requests for personnel action, copies of e-mail messages and handwritten notes.	1,550
June 16, 2006	Union Pacific (Omaha, NE)	On April 29th, an employee's laptop was stolen that contained data for current and former Union Pacific employees, including names, birth dates and Social Security numbers.	30,000
June 16, 2006	NY State Controller's Office (Albany, NY)	State controller data cartridge containing payroll data of employees who work for a variety of state agencies was lost during shipment. The data contained names, salaries, Social Security numbers and home addresses.	1,300
June 16, 2006	ING (Miami, FL)	Two ING laptops that carried sensitive data affecting of Jackson Health System hospital workers were stolen in December 2005. The computers, belonging to financial services provider ING, contained information gathered during a voluntary life insurance enrollment drive in December and included names, birth dates and Social Security numbers.	8,500
June 16, 2006	Univ. of Kentucky (Lexington, KY)	The personal data of current and former students including classroom rosters names, grades and Social Security numbers was reported stolen on May 26 following the theft of a professor's flash drive.	6,500
June 14, 2006	American Insurance Group (AIG), Indiana Office of Medical Excess, LLC (New York, NY)	The computer server was stolen on March 31 containing personal information including names, Social Security numbers, birth dates, and some medical and disability information.	930,000
June 14, 2006	Western Illinios Univ. (Macomb, IL)	On June 5th, a hacker compromised a University server that contained names, addresses, credit card numbers and Social Security numbers of people connected to the University. **UPDATE** (7/5/06): Number affected reduced from 240,000.	180,000
June 13, 2006	Minn. State Auditor (St. Paul, MN)	Three laptops possibly containing Social Security numbers of employees and recipients of housing and welfare benefits along with other personal information of local governments the auditor oversees have gone missing.	493
June 13, 2006	Oregon Dept. of Revenue (Salem, OR)	Electronic files containing personal data of Oregon taxpayers may have been compromised by an ex-employee's downloaded a contaminated file from a porn site. The "trojan" attached to the file may have sent taxpayer information back to the source when the computer was turned on.	2,200
June 13, 2006	U.S. Dept of Energy, Hanford Nucear Reservation (Richland, WA)	Current and former workers at the Hanford Nuclear Reservation that their personal information may have been compromised, after police found a 1996 list with workers' names and other information in a home during an unrelated investigation.	4,000
June 12, 2006	U.S. Dept. of Energy (Washington, D.C.)	Names, Social Security numbers, security clearance levels and place of employment for mostly contract employees who worked for National Nuclear Security Administration may have been compromised when a hacker gained entry to a computer system at a service center in Albuquerque, N.M. eight months ago.	1,502
June 11, 2006	Denver Election Commission (Denver, CO)	Records containing personal information on more than 150,000 voters are missing at city election offices. The microfilmed voter registration files from 1989 to 1998 were in a 500-pound cabinet that disappeared when the commission moved to new offices in February. The files contain voters' Social Security numbers, addresses and other personal information.	150,000
June 8, 2006	Univ. of Michigan Credit Union (Ann Arbor, MI)	Paper documents containing personal information of credit union members were stolen from a storage rooms. The documents were supposed to have been digitally imaged and then shredded. Instead, they	5,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

		were stolen and used to perpetrate identity theft.	
June 6, 2006	Univ. of Texas (El Paso, TX)	Students demonstrated that student body and faculty elections could be rigged by hacking into student information including Social Security numbers.	4,719
June 5, 2006	Internal Revenue Service (Washington, DC)	A laptop computer containing personal information of employees and job applicants, including fingerprints, names, Social Security numbers, and dates of birth, was lost during transit on an airline flight	291
June 2, 2006	Buckeye Community Health Plan (Columbus, OH)	Four laptop computers containing customer names, Social Security numbers, and addresses were stolen from the Medicaid insurance provider.	72,000
June 2, 2006	Ahold USA (Landover, MD) Parent company of Stop & Shop, Giant stores and Tops stores via subcontractor Electronic Data Systems (Plano, TX)	An EDS employee lost a laptop computer during a commercial flight that contained pension data of former employees of Ahold's supermarket chains including Social Security numbers, birth dates and benefit amounts.	Unknown
June 2, 2006	YMCA (Providence, RI)	Laptop computer containing personal information of members was stolen. The information included credit card and debit card numbers, checking account information, Social Security numbers, the names and addresses of children in daycare programs and medical information about the children, such as allergies and the medicine they take, though the type of stolen information about each person varies.	65,000
June 2, 2006	Humana (Louisville, KY)	Personal information of Humana customers enrolled in the company's Medicare prescription drug plans could have been compromised when an insurance company employee called up the data through a hotel computer and then failed to delete the file.	17,000 current and former Medicare enrollees
June 1, 2006	Miami University (Oxford, OH)	An employee lost a hand-held personal computer containing personal information of students who were enrolled between July 2001 and May 2006.	851
June 1, 2006	Ernst & Young (UK)	A laptop containing names, addresses and credit or debit card information of Hotels.com customers was stolen from an employee's car in Texas.	243,000
June 1, 2006	Univ. of Kentucky (Lexington, KY)	Personal information of current and former University of Kentucky employees including Social Security numbers was inadvertently accessible online for 19 days last month.	1,300
May 31, 2006	Humana (Louisville, KY)	On May 5, 2006, Medicare drug benefit applications were stolen from an insurance agent's unlocked car in Brooklyn Park, MN. Information included applicants' name, address, date of birth, Social Security number, and bank routing information.	268 Minnesota and North Dakota applicants
May 30, 2006	Texas Guaranteed Student Loan Corp. (Round Rock, TX) via subcontractor, Hummingbird (Toronto, Canada)	Texas Guaranteed (TG) was notified by subcontractor Hummingbird that on May 24, an employee had lost a piece of equipment containing names and Social Security numbers of TG borrowers. **UPDATE** (6/16/06): TG now says a total of 1.7 million people's information was compromised, 400,000 more than original estimate of 1.3 million.	1,300,000 plus 400,000 for total of 1,700,000
May 30, 2006	Florida Int'l Univ. (Miami, FL)	Hacker accessed a database that contained personal information, such as student and applicant names and Social Security numbers.	"thousands"
May 25, 2006	Vystar Credit Union (Jacksonville, FL)	Hacker gained access to member accounts "a few weeks ago" and stole personal information including names, addresses, birth dates, mother's maiden names, SSNs and/or email addresses.	Approx. 34,400 ("less than 10% of its 344,000 members")
May 24, 2006	Sacred Heart Univ. (Fairfield, CT)	It was discovered on May 8th that a computer containing personal information including names, addresses and Social Security numbers was breached.	Unknown
May 24, 2006	American Red Cross, St. Louis Chapter (St. Louis,	Dishonest employee had access to Social Security numbers of donors to call urging them to give blood again. The employee misused the persoal information of at least 3 people to perpetrate identity theft and had access to the personal information of 1 million donors.	1,000,000
May 23, 2006	Univ. of Delaware (Newark, DE)	Security breach of a Department of Public Safety computer server potentialy exposes names, Social Security numbers and driver's license numbers.	1,076

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

May 23, 2006	M&T Bank (Buffalo, NY)	Laptop computer, owned by PFPC, a third party company that provides record keeping services for M & T's Portfolio Architect accounts was stolen from a vehicle. The laptop contained clients' account numbers, Social Security numbers, last name and the first two letters of their first name.	Unknown
May 23, 2006	Butler Co. Dept. of Mental Retardation & Developmental Disabilities (Cincinatti, OH)	Three laptop computers were stolen "last month" from the agency's office. They contained personal information on mental health clients, including SSNs.	100 clients
May 23, 2006	Mortgage Lenders Network USA (Middletown, CT)	A former employee was arrested for extortion for attempting to blackmail his former employer for $6.9 million. He threatened to expose company files containing sensitive customer information - including customers' names, addressess, Social Security numbers, loan numbers, and loan types - if the company didn't pay him. He stole the files over the 16 months he worked there.	231,000
May 22, 2006	U.S. Dept. of Veteran's Affairs (Washington, DC) (800) 827-1000	On May 3, data of all American veterans who were discharged since 1975 including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses, were stolen from a VA employee's home. Theft of the laptop and computer storage device included data of 26.5 milliion veterans. The data did not contain medical or financial information, but may have disability numerical rankings. **UPDATE:** An additional 2.1 million active and reserve service members were added to the total number of affected individuals June 1st. **UPDATE** (6/29/06): The stolen laptop computer and the external hard drive were recovered. **UPDATE** (7/14/06): FBI claims no data had been taken from stolen computer. **UPDATE** (8/5/06): Two teens were arrested in the theft of the laptop. **UPDATE** (8/25/06): In an Aug. 25 letter, Secretary Nicholson told veterans of the decision to not offer them credit monitoring services. Rather the VA has contracted with a company to conduct breach analysis to monitor for "patterns of misuse."	28,600,000
May 19, 2006	American Institute of Certified Public Accountants (AICPA) (New York, NY)	An unencrypted hard drive containing names, addresses and Social Security numbers of AICPA members was lost when it was shipped back to the organization by a computer repair company.	330,000 [Updated 6/16/06]
May 19, 2006	Unknown retail merchant	Visa, MasterCard, and other debit and credit card numbers from banks across the country were stolen when a national retailer's database was breached. No names, Social Security numbers or other personal identification were taken.	Unknown
May 12, 2006	Mercantile Potomac Bank (Gaithersburg, MD)	Laptop containing confidential information about customers, including Social Security numbers and account numbers was stolen when a bank employee removed it from the premises, in violation of the bank's policies. The computer did not contain customer passwords, personal identification numbers (PIN numbers) or account expiration dates.	48,000
May 5, 2006	U.S. Dept. of Veteran's Affairs (Washington, D.C.)	A data tape disappeared from a VA facility in Indianapolis, IN that contained information on legal cases involving U.S. veterans and included veterans' Social Security numbers, dates of birth and legal documents. **UPDATE** (10/11/06): The VA's Office of the General Counsel is offering identity theft protection services to those affected by the missing tape.	16,500
May 5, 2006	Wells Fargo (San Francisco, CA)	Computer containing names, addresses, Social Security numbers and mortgage loan deposit numbers of existing and prospective customers may have been stolen while being delivered from one bank facility to another.	Unknown
May 4, 2006	Idaho Power Co. (Boise, ID)	Four company hard drives were sold on eBay containing hundreds of thousands of confidential company documents, employee names and Social Security numbers, and confidential memos to the company's CEO.	Unknown
May 4, 2006	Ohio University Hudson Health Center	Names, birth dates, Social Security numbers and medical information were accessed in records of students dating back to 2001, plus faculty, workers and regional campus students.	60,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

	(Athens, OH)		
May 2, 2006	Georgia State Government (Atlanta, GA)	Government surplus computers that sold before their hard drives were erased contained credit card numbers, birth dates, and Social Security numbers of Georgia citizens.	Unknown
May 2006	Ohio University (Athens, OH)	A breach was discovered on a computer that housed IRS 1099 forms for vendors and independent contractors for calendar years 2004 and 2005.	2,480
May 2006	Ohio University (Athens, OH)	A breach of a computer that hosted a variety of Web-based forms, including some that processed on-line business transactions. Although this computer was not set up to store personal information, investigators did discover files that contained fragments of personal information, including Social Security numbers. The data is fragmentary and it is not certain if the compromised information can be traced to individuals. Also found on the computer were 12 credit card numbers that were used for event registration.	Unknown
April 28, 2006	Ohio's Secretary of State (Cleveland, OH)	The names, addresses, and Social Security numbers of potentially millions of registered voters in Ohio were included on CD-ROMs distributed to 20 political campaign operations for spring primary election races. The records of about 7.7 million registered voters are listed on the CDs, but it's unknown how many records contained SSNs, which were not supposed to have been included on the CDs. **UPDATE** (9/15/06): A news report said that some SSNs still remain on the agency's Web site.	"Potentially millions of registered voters"
April 28, 2006	Dept. of Defense (Washington, DC)	Hacker accessed a Tricare Management Activity (TMA) public server containing personal information about military employees.	Unknown
April 27, 2006	MasterCard (Potentially UK only)	Though MasterCard refused to say how the breach occurred, fraudsters stole the credit card details of holders in a major security breach.	[2,000] Not included in total below.
April 27, 2006	Long Island Rail Road (Jamaica, NY)	Data tapes containing personal information including names, addresses, Social Security numbers and salary figures of "virtually everyone" who worked for the agency was lost by delivery contractor Iron Mountain while enroute. Data tapes belonging to the U.S. Department of Veteran's Affairs may also have been affected.	17,000
April 26, 2006	Purdue University (West Lafayette, IN)	Hacker accessed personal information including Social Security numbers of current and former graduate students, applicants to graduate school, and a small number of applicants for undergraduate scholarships.	1,351
April 26, 2006	Aetna -- health insurance records for employees of 2 members, including Omni Hotels and the Dept. of Defense NAF (Hartford, CT)	Laptop containing personal information including names, addresses and Social Security numbers of Dept. of Defense (35,253) and Omni Hotel employees (3,000) was stolen from an Aetna employee's car.	38,000
April 24, 2006	University of Texas' McCombs School of Business (Austin, TX)	Hackers accessed records containing names, biographical information and, in some cases, Social Security numbers and dates of birth of current and prospective students, alumni, faculty members, corporate recruiters and staff members.	197,000
April 24, 2006	Ohio University (Athens, OH)	Hackers accessed a computer system of the school's alumni relations department that included biographical information and 137,000 Social Security numbers of alum.	300,000
April 21, 2006	University of Alaska, Fairbanks (Fairbanks, AK)	A hacker accessed names, Social Security numbers, and partial e-mail addresses of current and former students, faculty, and staff.	38,941
April 21, 2006	Boeing (Seattle, WA)	A laptop was taken from a Boeing human resources employee at Sea-Tac airport. It contained SSNs and other personal information, including personnel information from the 2000 acquisition of Hughes Space and Communications	3,600 current and former employees
April 21, 2006	Ohio University Innovation Center (Athens, OH)	a server containing data including e-mails, patent and intellectual property files, and 35 Social Security numbers associated with parking passes was compromised.	Unknown
April 15, 2006	Scott County, IA	The Social Security numbers of people who obtained mortgages in the early 1990s are visible in	Unknown

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

		documents posted on the county's website. The county will redact the information at the individuals' request.	
April 14, 2006	NewTech Imaging (Honolulu, HI)	Records containing the names, Social Security numbers and birth dates of more than 40,000 members of Voluntary Employees Benefit Association of Hawaiiwere illegally reproduced at a copying business before they were to be put onto a compact disc for the State. Police later found the data on a computer that had been confiscated as part of a drug investigation.	40,000
April 14, 2006	Univ. of South Carolina (Columbia, SC)	Social Security numbers of students were mistakenly e-mailed to classmates.	1,400
April 12, 2006	Ross-Simons (Providence, RI)	Security breach exposed account and personal information of those who applied for its private label credit card. Information exposed includes private label credit card numbers and other personal information of applicants.	Unknown
April 9, 2006	University of Medicine and Dentistry of New Jersey (Newark, NJ)	Hackers accessed Social Security numbers, loan information, and other confidential financial information of students and alumni.	1,850
April 7, 2006	DiscountDomain Registry.com (Brooklyn, NY)	Exposed online. Domain registrants' personal information including usernames, passwords and credit card numbers were accessible online.	"thousands of domain name registrations"
April 6, 2006	Progressive Casualty Insurance (Mayfield Village, OH)	Dishonest insider accessed confidential information, including names, Social Security numbers, birth dates and property addresses on foreclosure properties she was interested in buying.	13
April 1, 2006	Con Edison (New York)	Con Edison shipped 2 cartridge tapes to JPMorgan Chase in upstate Binghamton so it could input data on behalf of the NY Dept. of Taxation and Finance. One tape was apparently lost containing employees' W-2 data, including names, addresses, SSNs, taxes paid and salaries.	15,000 Con Edison employees
Mar. 30, 2006	Marines (Monterey, CA)	Portable drive lost that contains personal information used for research on re-enlistment bonuses.	207,750
Mar. 30, 2006	Georgia Technology Authority (Atlanta, GA)	Hacker exploited security flaw to gain access to confidential information including Social Security numbers and bank-account details of state pensioners.	573,000
Mar. 30, 2006	Conn. Technical High School System (Middletown, CT)	Social Security numbers of students and faculty mistakenly distributed via email.	1,250
Mar. 24, 2006	CA State Employment Development Division (Sacramento, CA)	Computer glitch sends state Employment Development Division 1099 tax forms containing Social Security numbers and income information to the wrong addresses, potentially exposing those taxpayers to identity theft.	64,000
Mar. 24, 2006	Vermont State Colleges (VT)	Laptop stolen containing Social Security numbers and payroll data of students, faculty and staff associated with the five-college system from as long ago as 2000.	14,000
Mar. 23, 2006	Fidelity Investments (Boston, MA)	Stolen laptop containing names, addresses, birth dates, Social Security numbers and other information of 196,000 Hewlett Packard, Compaq and DEC retirement account customers was stolen.	196,000
Mar. 16, 2006	Bananas.com (San Rafael, CA)	Hacker accessed names, addresses, phone numbers and credit card numbers of customers.	274
Mar. 15, 2006	Ernst & Young (UK)	Laptop lost containing the names, dates of birth, genders, family sizes, Social Security numbers and tax identifiers for current and previous IBM, Sun Microsystems, Cisco, Nokia and BP employees exposed.	Unknown
Mar. 14, 2006	General Motors (Detroit, MI)	Dishonest insider keep Social Security numbers of co-workers to perpetrate identity theft.	100
Mar. 11, 2006	CA Dept. of Consumer Affairs (DCA) (Sacramento, CA)	Mail theft. Applications of DCA licensees or prospective licensees for CA state boards and commissions were stolen. The forms include full or partial Social Security numbers, driver's license numbers, and potentially payment checks.	"A small number"

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Mar. 8, 2006	Verizon Communications (New York, NY)	2 stolen laptops containing employees' personal information including Social Security numbers.	"Significant number"
Mar. 8, 2006	iBill (Deerfield Beach, FL)	Dishonest insider or possibly malicious software linked to iBill used to post names, phone numbers, addresses, e-mail addresses, Internet IP addresses, logins and passwords, credit card types and purchase amount online. Credit card account numbers, expiration dates, security codes, and SSNs were NOT included, but in our opinion the affected individuals could be vulnerable to social engineering to obtain such information.	[17,781,462] Not included in total below.
Mar. 5, 2006	Georgetown Univ. (Washington, D.C.)	Hacking. Personal information including names, birthdates and Social Security numbers of District seniors served by the Office on Aging.	41,000
Mar. 3, 2006	Metropolitan State College (Denver, CO)	Stolen laptop containing names and Social Security numbers of students who registered for Metropolitan State courses between the 1996 fall semester and the 2005 summer semester.	93,000
Mar. 2, 2006	Olympic Funding (Chicago, IL)	3 hard drives containing clients names, Social Security numbers, addresses and phone numbers stolen during break in.	Unknown
Mar. 2, 2006	Los Angeles Cty. Dept. of Social Services (Los Angeles, CA)	File boxes containing names, dependents, Social Security numbers, telephone numbers, medical information, employer, W-2, and date of birth were left unattended and unshredded.	[Potentially 2,000,000, but number unknown] Not included in number below.
Mar. 2, 2006	Hamilton County Clerk of Courts (OH)	SSNs, other personal data of residents posted on county Web site, were stolen and used to commit identity theft. **UPDATE** (9/28/06)**:** An identity thief was sentenced to 13 years in prison for the crimes. She stole 100 identities and nearly $500,000. The Web site now blocks access to court documents containing personal information.	[1,300,000] Not included in number below.
Mar. 1, 2006	Medco Health Solutions (Columbus, OH)	Stolen laptop containing Social Security numbers for State of Ohio employees and their dependents, as well as their birth dates and, in some cases, prescription drug histories.	4,600
Mar. 1, 2006	OH Secretary of State's Office	SSNs, dates of birth, and other personal data of citizens routinely posted on a State web site as part of standard business practice.	Unknown
Feb. 23, 2006	Deloitte & Touche (McAfee employee information)	External auditor lost a CD with names, Social Security numbers and stock holdings in McAfee of current and former McAfee employees.	9,290
Feb. 18, 2006	Univ. of Northern Iowa	Hacking. Laptop computer holding W-2 forms of student employees and faculty was illegally accessed.	6,000
Feb. 17, 2006	Calif. Dept. of Corrections, Pelican Bay (Sacramento, CA)	Inmates gained access to files containing employees' Social Security numbers, birth dates and pension account information stored in warehouse.	Unknown
Feb. 17, 2006	Mount St. Mary's Hospital (1 of 10 hospitals with patient info. stolen) (Lewiston, NY)	Two laptops containing date of birth, address and Social Security numbers of patients was stolen in an armed robbery in the New Jersey.	17,000
Feb. 16, 2006	Blue Cross and Blue Shield Jacksonville, FL	Contractor sent names and Social Security numbers of current and former employees, vendors and contractors to his home computer in violation of company policies.A judge today ordered a former computer consultant to reimburse the Jacksonville-based health insurer $580,000 for expenses related to his theft .	27,000
Feb. 15, 2006	Dept. of Agriculture	Inadvertently exposed Social Security and tax identification numbers in FOIA request.	350,000
Feb. 15, 2006	Old Dominion Univ.	Exposed online. Instructor posted a class roster containing names and Social Security numbers to a web site.	601
Feb. 13, 2006	Ernst & Young (UK)	Laptop stolen from employee's car with customers' personal information including Social Security numbers.	38,000 BP employees in addition to Sun, Cisco and IBM employees.

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Feb. 9, 2006	Unknown retail merchants, apparently OfficeMax and perhaps others.	Hacking. Debit card accounts exposed involving bank and credit union accounts nationwide (including CitiBank, BofA, WaMu, Wells Fargo). [3/13/06 Crime ring arrested.]	200,000, although total number is unknown.
Feb. 9, 2006	Honeywell International	Exposed online. Personal information of current and former employees including Social Security numbers and bank account information posted on an Internet Web site.	19,000
Feb. 4, 2006	FedEx	Inadvertently exposed. W-2 forms included other workers' tax information such as SSNs and salaries.	8,500
Feb. 1, 2006	Blue Cross and Blue Shield of North Carolina	Inadvertently exposed. SSNs of members printed on the mailing labels of envelopes with information about a new insurance plan.	600
Jan. 31, 2006	Boston Globe and The Worcester Telegram & Gazette	Inadvertently exposed. Credit and debit card information along with routing information for personal checks printed on recycled paper used in wrapping newspaper bundles for distribution.	240,000 potentially exposed
Jan. 27, 2006	State of RI web site (www.RI.gov)	Hackers obtained credit card information in conjunction with names and addresses.	4,117
Jan. 25, 2006	Providence Home Services (Portland, OR)	Stolen backup tapes and disks containing Social Security numbers, clinical and demographic information. In a small number of cases, patient financial data was stolen. **UPDATE:** (9/26/06) Providence Health System and the Oregon Attorney General have filed a settlement agreement. Providence will provide affected patients with free credit monitoring, offer credit restoration to patients who are victims of identity fraud, and reimburse patients for direct losses that result from the data breach. The company must also enhance its security programs.	365,000
Jan. 24, 2006	Univ. of WA Medical Center	Stolen laptops containing names, Social Security numbers, maiden names, birth dates, diagnoses and other personal data.	1,600
Jan. 23, 2006	Univ. of Notre Dame	Hackers accessed Social Security numbers, credit card information and check images of school donors.	Unknown
Jan. 21, 2006	California Army National Guard	Stolen briefcase with personal information of National Guardsmen including a "seniority roster," Social Security numbers and dates of birth.	"hundreds of officers"
Jan. 20, 2006	Univ. Place Conference Center & Hotel, Indiana Univ.	Hacking. Reservation information including credit card account number compromised.	Unknown
Jan. 17, 2006	City of San Diego, Water & Sewer Dept. (San Diego, CA)	Dishonest employee accessed customer account files, including SSNs, and committed identity theft on some individuals.	Unknown
Jan. 12, 2006	People's Bank	Lost computer tape containing names, addresses, Social Security numbers, and checking account numbers.	90,000
Jan. 9, 2006	Atlantis Hotel - Kerzner Int'l	Dishonest insider or hacking. Names, addresses, credit card details, Social Security numbers, driver's licence numbers and/or bank account data.	55,000
Jan. 2, 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown
Jan. 1, 2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen computers. Names, Social Security numbers, birthdates	700
Dec. 25, 2005	Iowa State Univ.	Hacking. Credit card information and Social Security numbers.	5,500
Dec. 25, 2005	Ameriprise Financial Inc. (Minneapolis, MN) (877) 267-7408	A laptop was stolen from an employee's car Christmas eve. It contained customers' names and Social Security numbers and in some cases, Ameriprise account information. **UPDATE** (08/06): The laptop was recovered by local law enforcement in the community where it was stolen. **UPDATE** (12/11/06): The company settled with the Massachusetts securities regulator in the office of the Secretary of State. Ameriprise agreed to hire an independent consultant to review its policies and procedures for employees' and contractors' use of laptops containing personal information. Ameriprise will pay the state regulator $25,000 for the cost of the investigation.	260,000
Dec. 22, 2005	Ford Motor Co.	Stolen computer. Names and SSNs of current and former employees.	70,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

Dec. 20, 2005	Guidance Software, Inc.	Hacking. Customer credit card numbers. **UPDATE** (4/3/07): The FTC came to a settlement agreement and final consent order against Guidance Software.	3,800
Dec. 16, 2005	La Salle Bank, ABN AMRO Mortgage Group	Backup tape with residential mortgage customers lost in shipment by DHL, containing SSNs and account information. **UPDATE** (12/20/05): DHL found the lost tape.	[2,000,000] Not included in total below.
Dec. 16, 2005	Colorado Tech. Univ.	Email erroneously sent containing names, phone numbers, email addresses, Social Security numbers and class schedules.	1,200
Dec. 12, 2005	Sam's Club/Wal-Mart	Exposed credit card data at gas stations.	Unknown
Dec. 7, 2005	Idaho State University, Office of Institutional Research (Pocatello, ID) Contact Information Technology Services, (208) 282-2872	ISU discovered a security breach in a server containing archival information about students, faculty, and staff, including names, SSNs, birthdates, and grades.	Unknown
Dec. 6, 2005	WA Employment Security Dept.	Stolen laptop. Names, SSNs and earnings of former employees.	530
Dec. 2, 2005	Cornell Univ.	Hacking. Names, addresses, SSNs, bank names and acct. numbers.	900
Dec. 1, 2005	Firstrust Bank	Stolen laptop	100,000
Dec. 1, 2005	Univ. of San Diego (San Diego, CA)	Hacking. Faculty, students and employee tax forms containing SSNs	7,800
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer, Theft 10/16/05	13,000
Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 8, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves. Total affected now reaches 163,000 (See Feb. 15 & Sept. 16)	[Total later revised to 163,000 -- see 2/15/05 above]
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer	50,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 12, 2005	Ohio State Univ. Medical Center	Exposed online. Appointment information including SSN, DOB, address, phone no., medical no., appointment reason, physician.	2,800
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 22, 2005	City University of New York	Exposed online	350

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights CLEARINGHOUSE

Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop (7/24/05) with mortgage data	9,000
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05) (Alpharetta, GA)	ID thieves accessed; also misuse of IDs & passwords.	[Total later revised to 163,000 -- see 2/15/05 above]
Sept. 15, 2005	Miami Univ.	Exposed online	21,762
Sept. 10, 2005	Kent State Univ.	Stolen computers	100,000
Aug. 30, 2005	J.P. Morgan Chase & Co. (Dallas, TX)	Stolen laptop (Aug. 8) containing personal and financial account information of customers of its private bank.	Unknown
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking	154
Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen Laptop	3,851
Aug. 22, 2005	Air Force	Hacking	33,300
Aug. 19, 2005	Univ. of Colorado	Hacking	49,000
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking	900
Aug. 10, 2005	Univ. of North Texas	Hacking	39,000
Aug. 9, 2005	Sonoma State Univ.	Hacking	61,709
Aug. 9, 2005	Univ. of Utah	Hacking	100,000
Aug. 2, 2005	Univ. of Colorado	Hacking	36,000
July 31, 2005	Cal Poly-Pomona	Hacking	31,077
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking	33,000
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking	9,613
July 21, 2005	Univ. of Colorado-Boulder	Hacking **UPDATE** (08/20/2005) The number of students affected was increased from an estimate of 42,000 to 49,000.	49,000
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens"exposed
July 7, 2005	Mich. State Univ.	Hacking	27,000
July 6, 2005	City National Bank	Lost backup tapes	Unknown
July 1, 2005	Univ. of CA, San Diego	Hacking	3,300
June 30, 2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
June 29, 2005	Bank of America	Stolen laptop	18,000
June 28, 2005	Lucas Cty. Children Services (OH)	Exposed by email	900
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 22, 2005	East Carolina Univ.	Hacking	250

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000
June 17, 2005	Kent State Univ.	Stolen laptop	1,400
June 16, 2005	CardSystems	Hacking	40,000,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
May 30, 2005	Motorola	Computers stolen	Unknown
May 28, 2005	Merlin Data Services (Kalispell, MT)	Bogus acct. set up	9,000
May 27, 2005	Cleveland State Univ. (Cleveland, OH).	Stolen laptop **UPDATE** (12/24): CSU found the stolen laptop	[44,420] Not included in total below
May 26, 2005	Duke Univ. (Durham, NC)	Hacking	5,500
May 25, 2005	North Carolina Div. of Motor Vehicles (Greensboro, NC)	On Feb. 10, an employee downloaded addresses of 3.8 million people but was detected and stopped before being able to retrieve more sensitive information such as driver's license numbers.	None
May 19, 2005	Valdosta State Univ. (GA)	Hacking	40,000
May 18, 2005	Jackson Comm. College (MI)	Hacking	8,000
May 18, 2005	Univ. of Iowa	Hacking	30,000
May 16, 2005	Westborough Bank (Westborough, MA)	Dishonest insider	750
May 12, 2005	Hinsdale Central High School (Hinsdale, IL)	Hacking	2,400
May 11, 2005	Stanford Univ. (Stanford, CA)	Hacking	9,900
May 7, 2005	Dept. of Justice (Washington, D.C.)	Stolen laptop	80,000
May 5, 2005	Purdue Univ. (West Lafayette, IN)	Hacking	11,360
May 4, 2005	CO. Health Dept.	Stolen laptop	1,600 (families)
May 2, 2005	Time Warner (New York, NY)	Lost backup tapes	600,000
April 29, 2005	Oklahoma State Univ.	Missing laptop	37,000
April 28, 2005	Georgia Southern Univ.	Hacking	"tens of thousands"
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
April 26, 2005	Mich. State Univ's Wharton Center	Hacking	40,000

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

April 26, 2005	Christus St. Joseph's Hospital (Houston, TX)	Stolen computer	19,000
April 21, 2005	Carnegie Mellon Univ. (Pittsburg, PA)	Hacking	19,000
April 20, 2005	Ameritrade (Bellevue, NE)	Lost backup tape	200,000
April 18, 2005	DSW/ Retail Ventures (Columbus, OH)	Hacking	Additional 1,300,000
April 15, 2005	CA Dept. of Health Services	Stolen laptop	21,600
April 14, 2005	Polo Ralph Lauren/HSBC (New York, NY)	Hacking **UPDATE** (07/10/07): U.S. Secret Service agents found Ralph Polo Lauren customers' credit card numbers in the hands of Eastern European cyber thieves who created high-quality counterfeit credit cards. Victims are from the U.S., Europe, Asia and Canada, among other places, Several Cuban nationals in Florida were arrested with more than 200,000 credit card account numbers.	180,000
April 14, 2005	Calif. Fastrack	Dishonest Insider	4,500
April 12, 2005	LexisNexis (Dayton, OH)	Passwords compromised **UPDATE** (06/30/06): Last week, five men were arrested in connection with this breach.	Additional 280,000
April 11, 2005	Tufts University (Boston, MA)	Hacking	106,000
April 8, 2005	Eastern National	Hacker	15,000
April 8, 2005	San Jose Med. Group (San Jose, CA)	Stolen computer	185,000
April 6, 2005	University of California, San Francisco	A server in the accounting and personnel departments was hacked. It contained information on 7,000 students, faculty, and staff members. The affected individuals were notified March 23.	7,000
April 5, 2005	MCI (Ashburn, VA)	Stolen laptop	16,500
April 5, 2005	Univ. of CA, Davis (Davis, CA)	The names and Social Security numbers of students, faculty, visiting speakers and staff may have been compromised when a hacker accessed a main computer.	1,100
March 25, 2005	Purdue University (West Lafayette, IN)	Computers in the College of Liberal Arts' Theater Dept. were hacked, exposing personal information of employees, students, graduates, and business affiliates.	1,200 (not included in total because news stories are not clear if SSNs or financial information were exposed)
March 23, 2005	Univ. of CA. (San Francisco, CA)	Hacking	7,000
March 22, 2005	Calif. State Univ. (Chico, CA)	Hacking	59,000
March 20, 2005	Northwestern Univ. (Evanston, IL)	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas (Las Vegas, NV)	Hacking	5,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer. **UPDATE:** The computer was later recovered.	[8,900] Not included

A Chronology of Data Breaches

Posted April 20, 2005
Updated August 17, 2007

Privacy Rights Clearinghouse

			in total below
March 11, 2005	Univ. of CA, Berkeley (Berkeley, CA)	Stolen laptop	98,400
March 11, 2005	Kaiser Permanente (Oakland, CA)	A disgruntled employee posted informaton on her blog noting that Kaiser Permanente included private patient information on systems diagrams posted on the Web. **UPDATE** (6/21/2005): The California Department of Managed Health Care fined Kaiser $200,000 for exposing the confidential health information.	140
March 11, 2005	Boston College (Boston, MA)	Hacking	120,000
March 10, 2005	LexisNexis (Dayton, OH)	Passwords compromised **UPDATE** (06/30/06): Last week, five men were arrested in connection with this breach.	32,000
March 8, 2005	DSW/Retail Ventures (Columbus, OH)	Hacking	100,000
Feb. 25 , 2005	Bank of America (Charlotte, NC)	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx (Miramar, FL)	Exposed online	25,000
Feb. 18, 2005	Univ. of Chicago Hospital (Chicago, IL)	Dishonest insider	85
Feb. 15, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves. The initial number of affected records was estimated at 145,000 but was later revised to 163,000. **UPDATE** (1/26/06): ChoicePoint settled with the Federal Trade Commission for $10 million in civil penalties and $5 million for consumer redress. **UPDATE** (12/06/06): The FTC announced that victims of identity theft as a result of the data breach who had out-of-pocket expenses can now be reimbursed. The claims deadline is Feb. 4, 2007.	163,000 **UPDATE** (06/24/07): Starting Dec. 2006, the FTC began mailing claims forms to victims of the breach. Its Web site provides information about the claims process. Deadline is Aug. 18, 2007. Victims can be reimbursed for out-of-pocket expenses resulting from identity theft connected to the breach. Call (888) 884-8772, or email cpredress@ftc.gov.
Feb. 12, 2005	Science Applications International Corp. (SAIC) (San Diego, CA)	On Jan. 25 thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and current employees. Stolen information included names, NNS, addresses, phone numbers and records of financial transactions.	45,000 employees
Jan. 22, 2005	University of Northern Colorado (Greeley, CO)	A hard drive was apparently stolen. It contained information on current and former University employees and their beneficiaries -- name, date of birth, SSN, address, bank account and routing number..	30,000
Jan. 18, 2005	Univ. of CA, San Diego (San Diego, CA)	A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.	3,500
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
April 00, 2005	Georgia DMV	Dishonest insider	465,000
2005	U.S. Dept. of Veteran's Affairs	A laptop being stored in the trunk of a car was stolen in Minneapolis, Minnesota. 2 people later reported	66

(Exact date Unknown]	(Washington, D.C.)	identity fraud problems.	
TOTAL number of records containing sensitive personal information involved in security breaches			**159,072,498**