

2005 Disclosures of U.S. Data Incidents

(At least 152 incidents have been disclosed, potentially affecting more than 57.7 million individuals)

<u>Date</u>	<u>Entity</u>	<u>Affected</u>
1/3/05	George Mason University – Officials discover that hackers had accessed private information and Social Security numbers on students and staff.	30,000
1/6/05	University of Kansas – Administrators send letters to individuals whose personal information, including Social Security numbers, passport numbers, countries of origin, and birthdates, might have been compromised when a hacker accessed a server in November 2004.	1,400
1/05	Christus St. Joseph Hospital, Houston Texas – Published reports on 4/26 said the hospital had sent letters to 16,000 patients saying their medical records and SSNs may have been compromised due to the theft of a computer in a January burglary.	16,000
1/05	Kaiser Permanente – Health care company in March begins notifying patients that a disgruntled former employee had posted confidential information about them on the Internet; U.S. Office of Civil Rights had discovered the breach in January.	140
1/18/05	University of California at San Diego – Officials reveal a mid-November breach may have compromised names and SSNs of students and alumni.	3,500
1/20/05	University of Northern Colorado -- University announces the apparent theft of a computer hard drive containing names, addresses, SSNs, bank account numbers, dates of birth and pay schedules for students and staff members and potentially their beneficiaries.	30,000
1/25/05	Science Applications International (SAIC) -- Desktop computers were stolen from the offices of SAIC, a research and engineering company, compromising personal information of current and past stockholders.	Unknown/Not disclosed
1/26/05	GMAC Financial Services – News report says company begins “quietly” notifying customers on March 12 that personal data (names, addresses, dates of birth, SSNs, credit scores, marital status and gender) may have been compromised in the theft of two laptop computers from an employee’s car at a regional office near Atlanta.	200,000
1/27/05	Purdue University – An unknown person or group accessed a computer in the College of Liberal Arts' Theatre Division containing names and SSNs of faculty, staff, students, alumni and business affiliates.	1,200

2/05	University of California, San Francisco	7,000
	– University acknowledges in March that hackers breached a server used by its accounting and personnel departments in February, exposing names and SSNs of students, faculty and staff members.	
2/2/05	Indiana University	Unknown/Not disclosed
	– Officials reveal that the F.B.I. and campus police are investigating a computer security breach that left employees' personal information vulnerable. It is unknown how many have been affected.	
2/10/05	North Carolina Division of Motor Vehicles	3.8 million
	– North Carolina DMV confirms on May 24 it is investigating a state contract worker who downloaded the addresses of more than 3.8 million people from a DMV database. The State Bureau of Investigation said it believes it stopped the employee before driver's license numbers, SSNs and other information could be compromised.	
2/14/05	ChoicePoint	157,000
	– Makes notifications stemming from customer fraud which may have exposed consumers' personal data; number updated periodically from initial 145,000.	
2/20/05	T-Mobile	400
	– Mobile phone accounts of Paris Hilton and 400 T-Mobile customers compromised by hackers.	
2/23/05	PayMaxx	25,000
	– Online payroll service provider shuts down its automated W-2 site after a researcher claims data on more than 25,000 W-2 forms was exposed.	
2/24/05	Westlaw *	Potential for "Millions"
	– Accused by U.S. Sen. Charles Schumer of having "egregious loopholes" in one of its Internet data services that would allow thieves to harvest SSNs and financial identities of millions of people.	
2/25/05	Bank of America	1.2 million
	– Announced it had lost computer data tapes containing personal information on federal employees, including some members of the U.S. Senate.	
3/8/05	DSW Shoes	1.4 million
	– Announced credit card information from customers of more than 100 DSW Shoe Warehouse stores was stolen from company database; announces on 4/18 the number of affected consumers could be 1.4 million.	
3/05	Automatic Data Processing	1,000
	– Corporate payroll and benefits services company mistakenly distributes postcards imprinted with SSNs to more than 1,000 employees of Adecco Employment Services, an HR firm.	

3/07/05	Nevada Department of Motor Vehicles	8,800
	– Personal information compromised when thieves stole a computer from a Nevada DMV office. The computer and other license-making supplies are mysteriously found June 1 at a construction site in Las Vegas.	
3/8/05	Harvard University	200
	– Intruder gains access to admission systems and helped applicants log on to learn whether they had been accepted weeks before they were to find out.	
3/9/05	Reed Elsevier, Seisint Unit (LexisNexis)	310,000
	– Announced that hackers gained access to sensitive personal information of about 32,000 U.S. citizens on databases owned by Reed Elsevier; later updates the number of potentially affected consumers to 310,000.	
3/11/05	Boston College	120,000
	– Announced that hackers had accessed personal information of alumni in a computer system used for fund-raising.	
3/11/05	University of California-Berkeley	100,000
	– Laptop computer stolen from a graduate division office contained the names and Social Security numbers of nearly 100,000 individuals.	
3/14/05	California State University, Chico	59,000
	– Hackers broke into a computer system that contained names and SSNs of current, former and prospective students, as well as faculty and staff.	
3/18/05	University of Nevada, Las Vegas	5,000
	– Administrators reveal that a hacker had been accessing the personal information of international students.	
3/23/05	Mutual funds	Unknown/Not disclosed
	– <i>Wall Street Journal</i> reveals numerous mutual funds reported data security breaches, including Armada Funds; Pimco, a unit of German insurance giant Allianz AG; The Dreyfus unit of Mellon Financial Corp.; Bank of America Corp.'s Columbia Funds unit; Nuveen Investments; The First American Funds unit of U.S. Bancorp; AmSouth Bancorp's fund unit; CNI Charter fund unit of City National Bank of Los Angeles.	
3/25/05	Northwestern University	21,000
	– Hackers broke into a graduate school server, exposing the Social Security numbers of students, faculty, and alumni.	
3/28/05	San Jose Medical Group	185,000
	– Two computers stolen containing patient billing information, including names, addresses, Social Security numbers and confidential medical information.	
3/28/05	University of Chicago Hospital	Unknown/Not disclosed
	– Announced an employee had been selling patient records.	

3/05	Idaho State University (Pocatello)	100
	– Discovers that SSNs of students had been accessible to the public for more than three years on the university's Web site.	
4/05	MCI	16,500
	– Long-distance phone company acknowledges in a 5/23 article in The Wall Street Journal the theft in April of a laptop computer that contained names and SSNs of current and former employees.	
4/8/05	Eastern National (vendor for National Park Service).....	15,000
	– Hacker infiltrated its "eParks.com" computer system and may have gained access to customer names, credit card numbers and billing addresses.	
4/10/05	Carnegie Mellon University, Pittsburgh	19,000
	– Published reports on 4/21 said the university had sent letters to students, employees and graduates that their SSNs and other personal information was compromised in a breach of the school's computer network that was discovered on 4/10.	
4/12/05	Tufts University	106,000
	– Begins notifying 106,000 alumni about "abnormal activity" on a computer that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers.	
4/13/05	Polo Ralph Lauren / HSBC North America	180,000
	– Credit card issuer begins notifying consumers (who used General Motors-branded MasterCards to make purchases at Polo Ralph Lauren) that criminals may have obtained access to their credit-card information.	
4/15/05	California Department of Health Services	21,600
	– Department confirms on May 27 the theft of a laptop computer that contained personal information (names, SSNs, health information) for 21,600 recipients of Medi-Cal services. The computer was stolen from the trunk of a car of an employee of a company that provides data services to the state.	
4/18/05	Internal Revenue Service *	Potential for "Millions"
	– GAO reports computer-security flaws expose millions of taxpayers to ID theft. IRS confirms in June an investigation into potential data theft.	
4/19/05	Ameritrade	200,000
	– Online discount broker reported it has notified current and former customers that it has lost a backup computer tape containing their personal information.	
4/23/05	Georgia Southern University, Statesboro, Ga.	Potential for "Thousands"
	– AP reports on 4/28 that hackers broke into a GSU server that contained thousands of credit card and Social Security numbers.	

4/26/05	Michigan State University, Wharton Center 40,000 – Performing arts center says it learned of an intrusion on April 26 into a server that plays a role in credit card processing for ticket sales. The incident is not made public until media reports reveal the breach on May 5.	40,000
4/26/05	Foster Wheeler, Clinton, N.J. 6,700 – Engineering/construction company writes to employees, retirees, advising them that a hacker broke into the company’s computer system in February and might have stolen personal data, including SSNs and bank deposit information.	6,700
4/28/05	Wachovia, Bank of America, PNC Bank of Pittsburgh, Commerce Bank 680,000 – NBC reports bank managers/employees sold personal data of account holders.	680,000
4/28/05	Georgia Technology Authority (driver’s license data) 465,000 – Computer programmer arrested, charged with downloading state driver’s license information – including names, addresses, driver’s license numbers and possibly SSNs; “hundreds of thousands” of drivers may be affected.	465,000
4/28/05	Oklahoma State University 23,000 – University confirms theft of a laptop computer that contained SSNs, genders, ethnicities, class levels and e-mail addresses of “the majority” of students who attended OSU over the past three years (23,000 annual enrollment).	23,000
4/29/05	Florida International University Unknown/Not disclosed – Orlando Sun-Sentinel reports “recent computer break-in” potentially compromises personal data of students, professors and staffers. School says electronic intruders apparently dialed into FIU’s computers from Europe.	Unknown/Not disclosed
5/2/05	Time Warner 600,000 – Company announces that data on current and former employees stored on computer back-up tapes was lost by an outside storage company.	600,000
5/4/05	Colorado Department of Health 1,600 – News reports reveal the theft of a laptop computer containing medical and other information about more than 1,600 children.	1,600
5/5/05	Purdue University 11,360 – Computers breached over a 17-day period, compromising personal information of current and former employees.	11,360
5/5/05	Arbella Mutual Insurance Unknown/Not disclosed – Boston Globe reports an Arbella Web site mistakenly offered unrestricted access to names, addresses, dates of birth, drivers license numbers and history, and SSNs, including Boston Mayor Menino and Mass. Gov. Romney.	Unknown/Not disclosed

5/7/05	U.S. Department of Justice	80,000
	– Justice Department says a computer containing the names and government credit card numbers for DOJ personnel was stolen between May 7-9 from Omega World Travel, which handles business travel for the department. DOJ doesn't believe personal information (SSNs, etc.) was compromised.	
5/11/05	Stanford University	10,000
	– University confirms breach of computer network, stealing SSNs and other personal information of recruiters and students.	
5/12/05	Merlin Information Services	9,000
	– Kalispell, Mont., data company acknowledges names, addresses, SSNs were compromised in fraudulent access incident(s) in March/April.	
5/12/05	Hinsdale Central High School, Chicago	2,400
	– Two students are accused of hacking into a school database that contained the Social Security numbers of all of the school's students and staff.	
5/16/05	Westborough (Mass.) Bank	750
	– Bank begins notifying customers that a former bank employee may have given SSNs and other confidential account information to a convicted felon.	
5/17/05	Valdosta (Ga.) State University	40,000
	– University confirms breach of computer server containing SSNs, other information for multipurpose identification and on-line debit cards of students and employees. AP reports on 5/21 that 40,000 people could be affected.	
5/18/05	Jackson (Mich.) Community College	8,000
	– University confirms breach of computer system, potentially compromising employee and student SSNs.	
5/18/05	University of Iowa	30,000
	– University confirms breach of campus book store computer system, potentially compromising employee and student IDs, credit card numbers.	
5/23/05	Brigham Young University	600
	– University confirms a hacker in April monitored e-mail activity and recorded keystrokes of students who used four computers in an open-access lab.	
5/26/05	Duke University Medical Center	14,000
	– School says (on 6/3) that a hacker broke into its computer system and stole names, passwords and partial SSNs of employees, physicians and others.	
5/27/05	Cleveland State University	44,000
	– University confirms theft of a laptop computer from its admissions office, compromising students' addresses and SSNs.	

5/28-30/05	Motorola	30,000
	– Confirms theft of computers from HR services provider, Affiliated Computer Services, exposing its U.S. employees' personal data, including SSNs.	
6/2/05	Jackson High School, Jackson Township, Ohio	Unknown/Not disclosed
	– Two seniors convicted of illegally accessing school computers to change grades and acquire teachers' SSNs, credit card information and addresses.	
6/3/05	Polk Community College, Winter Park, Fla.	At least 3
	– Professor arrested for using students' names, SSNs to obtain department store credit cards. He allegedly had asked students to provide the data on a sign-up sheet for his class.	
6/6/05	CitiFinancial	3.9 million
	– Consumer financial division of Citigroup begins notifying customers that computer tapes containing their SSNs and account data were apparently lost in transit via UPS some time between May 2 and May 20.	
6/10/05	Federal Deposit Insurance Corp. (FDIC)	6,000
	– Begins notifying current and former employees of a 2004 breach that may have compromised their names, SSNs, DOBs, salaries and employment information.	
6/14/05	Medica Health Plans (Minnetonka, Minn.)	1.2 million
	– Confirms that hackers twice stole sensitive and confidential data from its computer system in January and shut down parts of the system on four other occasions, exposing members' SSNs, addresses, DOBs, employment information and names of relatives.	
6/17/05	Kent State University	1,400
	– Acknowledges the theft on June 14 of a laptop computer from an employee's car, which contained names and Social Security numbers of about 1,400 current and past school employees.	
6/17/05	University of Hawaii	150,000
	– Acknowledges that two identity theft suspects had gained fraudulent access to the school's database, exposing SSNs, addresses and phone numbers of students, faculty, staff and library patrons between 1999 and 2003.	
6/17/05	MasterCard International	40 million
	– Confirms hacking (discovered in late May) at CardSystems Solutions -- which handles transfer of payments between banks for consumer transactions -- exposes names, account numbers and verification codes of MasterCard, Visa, Discover, American Express card holders.	
6/22/05	Eastman Kodak	5,800
	– Confirms it has begun notifying former employees that names, SSNs, birthdates and other information was on a laptop computer stolen from a consultant's car.	

6/22/05	East Carolina University	250
	– Confirms May 2005 breach of an Internet server that contained SSNs, other personal information of students; says it believes the breach was limited to students and applicants in one department.	
6/24/05	University of Connecticut	72,000
	– Confirms it has discovered a computer-hacking program had been placed in a server at the school in 2003, compromising names, SSNs, DOBs, phone numbers and addresses of students, faculty and staff.	
6/27/05	Michigan State University, Human Resources Dept.	Unknown/Not disclosed
	– Media reports on 7/7 reveal a breach within the human resources department that may have exposed SSNs of all university employees and retirees.	
6/28/05	Lucas County (Ohio) Children Services	900
	– Confirms current and former employees' names, SSNs, phone numbers contained in a personnel database had been e-mailed to outside computer.	
6/29/05	Virginia Department of Criminal Justice Services	3,500
	– Confirms notifications due to potential theft of names, SSNs and phone numbers of people who had filed applications for jobs at the agency.	
6/30/05	Ohio State University Medical Center	15,000
	– Confirms notifications to patients whose names and billing information was contained on a laptop computer stolen in April from a consultant's office.	
7/1/05	University of California at San Diego	3,300
	– Confirms fourth hacking since April 2004. SSNs, drivers license, credit card numbers of students, staff and faculty compromised in incident in April.	
7/1/05	Blue Cross and Blue Shield of North Carolina *	Unknown/Not disclosed
	– Files lawsuit against ProCare, a private group, for allegedly posting illegally obtained internal documents on the Internet (this incident is not currently included in our list as a "breach" pending more clarification).	
7/5/05	City National Bank, Los Angeles	Unknown/Not disclosed
	– "Banker to the stars" confirms account holders' names, SSNs, account numbers and other info was on two backup data tapes that were lost in April.	
7/5/05	Michigan State University, College of Education	27,000
	– Confirms discovery in April of a breach of a server in the College of Education that exposed students' names, addresses, SSNs, other info.	
7/8/05	University of Southern California	270,000
	– Confirms a hacker (since 1997) may have gained access to students' names, addresses and SSNs due to a flaw in an online application database.	

7/8/05	Blue Cross Blue Shield of Arizona	57,000
	– Confirms customers' addresses, SSNs, DOBs, phone numbers were on backup tapes stolen 6/29 from Arizona Biodyne, a managed care company.	
7/14/05	University of Colorado	42,000
	– Breach of Wardenburg Health Center computer server exposes names, SSNs, ID numbers, addresses, birthdates of students, faculty, staff, visitors.	
7/14/05	University of Colorado	900
	– Breach of server in the Visual Resource Center of the College of Architecture and Planning exposes names and SSNs of students and faculty.	
7/15/05	University of Delaware	343
	– Confirms the December 2004 theft of three computers, one of which contained Department of Communications students' names, SSNs.	
7/18/05	Iowa State University	4,700
	– Confirms the 7/6 discovery of a breach of its network exposing the SSNs and/or credit card numbers of Alumni Association customers since 2004.	
7/21/05	San Diego County Employees Retirement Association	32,000
	– Discovers unauthorized access of two computer servers containing names, SSNs, birthdates, addresses of current and former county employees.	
7/25/05	St. John's Regional Medical Center, Joplin, Mo.	27,000
	– Acknowledges 7/7 theft of two computers containing patients' names, dates of birth and some medical account numbers.	
7/26/05	California State University, Dominguez Hills	9,613
	– Discovers the unauthorized access of three desktop computers containing names and SSNs of students.	
7/27/05	University of Colorado	36,000
	– Discovers breach of computer server (used to issue identification cards) exposing names, SSNs, photos of students, former students, faculty, staff.	
7/29/05	Austin Peay State University, Clarksville, Tenn.	1,500
	– Confirms exposure of students' names, SSNs, other personal info due to a problem with the search function on the school's Web site.	
7/29/05	Cal Poly Pomona	31,077
	– Confirms 6/29 hacking of two computer servers, compromising names and SSNs of current and former faculty, staff, students and university applicants.	
8/3/05	Anderson College, Anderson, S.C.	834
	– A bag containing documents bearing students SSNs, gender and dates of birth is discovered off campus; college investigating possibility of theft.	

8/4/05	Pennsylvania Unified Judicial System	Unknown/Not disclosed
	– Confirms “five to 10 minute access” via a Web site compromised SSNs, other confidential information of defendants on statewide computer system.	
8/8/05	Sonoma State University, Rohnert Park, Calif.	61,709
	– Confirms unauthorized access of computer system had exposed names and SSNs of all students, faculty, staff and applicants from 1995 to 2002.	
8/8/05	University of North Texas, Denton, Texas	38,607
	– Discloses “hacking” of system exposing names, SSNs, student IDs, phone numbers of current, former and prospective students from 1999 to 2005.	
8/8/05	Huntington National Bank, Toledo, Ohio	6,000
	– Confirms distribution of notification letters due to theft of account information, including names, SSNs, signatures, account numbers of local customers.	
8/8/05	J.P. Morgan Private Bank	Unknown/Not disclosed
	– Distributes letters on Aug. 25 advising of theft of a computer from its Dallas offices containing personal and financial information about its wealthy clients.	
8/9/05	University of Utah	100,000
	– Confirms notification under way due to apparent “hacking” of a computer server containing names, SSNs of former employees from 1970 to 2003.	
8/9/05	Iowa Student Loan Program	165,000
	– Learns from a vendor about a missing compact disc containing names, SSNs and states of residence of borrowers from the program.	
8/9-10/05	Aims Community College, Greeley, Colo.	2,000
	– Confirms on Sept. 12 the theft of a computer containing names and SSNs of students in fire science and emergency services programs.	
8/10/05	Austin Peay State University, Clarksville, Tenn.	1,280
	– Confirms additional exposure of students’, vendors’ names, SSNs, addresses, phone numbers, other info due to problem with school’s Web site.	
8/10/05	California State University, Stanislaus	877
	– Discovers a breach of a computer file server containing names, SSNs of student workers.	
8/18/05	U.S. Air Force	33,000
	– Confirms “personal information” of officers and enlisted personnel was stolen from its online Assignment Management System in May or June.	
8/19/05	University of Colorado	49,000
	– Confirms breach of computer server used by Registrar’s Office, exposing names, SSNs, addresses, phone numbers of current and former students.	

8/19/05	ChartOne / University of Florida Health Sciences Center	3,851
	– Confirms theft of laptop computer (on or about Aug. 1) containing patients' names, SSNs, dates of birth and medical record numbers.	
8/20-21/05	U.S. Army, Fort Carson, Colo.	15,000
	– Confirms on Sept. 12 the theft of four computer hard drives containing names, SSNs and personal records of soldiers processed at Fort Carson.	
8/21-22/05	Kent State University	100,000
	– Confirms on Sept. 9 the theft of five computers containing names and SSNs of current and former students and professors.	
08/28/05	Stark State College of Technology (Jackson Township, Ohio)	Unknown/Not disclosed
	– Acknowledges software “glitch” allowed students to inadvertently view personal information of other students, including SSN, GPA, course loads.	
08/29/05	California State University Chancellor’s Office	154
	– Confirms unauthorized access (via virus) of computer exposing names, SSNs of individuals who received student financial aid, two administrators.	
8/31/05	Blue Cross Blue Shield of Florida *	194
	– Confirms insurance subsidiary sent letters to policyholders (all BCBS employees, relatives or retirees) with their SSNs printed on the envelope.	
9/07/05	Children’s Health Council, Palo Alto, Calif.	6,700
	– Discovers theft of a backup tape containing names, SSNs and other personal information on current and former clients and employees.	
9/12/05	Miami University (Ohio)	21,762
	– Acknowledges it had removed students’ SSNs and grades from a Web folder where they had been accessible via the Internet for nearly three years.	
9/14/05	North Fork Bank, Melville, N.Y.	9,000
	– Distributes letters notifying mortgage loan customers about the theft in July of a laptop computer containing their personal information (perhaps not SSNs).	
9/19/05	University of Georgia	1,600
	– Discovers unauthorized computers access, believed to be from another country, which exposed names, SSNs of current and former employees.	
9/21/05	City College of New York	9,000
	– Acknowledges that CUNY Law School students’ names, SSNs and other personal info were accidentally posted on a university Web site.	
9/22/05	ChoicePoint	5,000
	– Makes notifications stemming from misuse of IDs/passwords by customers, including a police department, insurance company, P.I. firm and others.	

9/22/05	World Trade Center Medical Monitoring Program	10,000
	– Sends letters re: 7/10 theft of computer from Mt. Sinai Hospital containing SSNs, other info of Ground Zero police/fire rescue and cleanup workers.	
9/27/05	RBC Dain Rauscher	100
	– Notifies customers of illegal access to customer data by former employee who wrote anonymous letters saying he/she had compromised data.	
9/23/05	Bank of America	Unknown/Not disclosed
	– Sends letters re: 8/29 theft of laptop computer containing Visa Buxx users' names, account numbers, routing transit numbers and credit card numbers.	
10/05/05	Wilcox Memorial Hospital, Kauai, Hawaii	130,000
	– Discloses on 10/17 the theft of a computer hard drive containing patients' names, addresses, SSNs and medical record numbers.	
10/07/05	Montclair State University, Montclair, N.J.	9,100
	– Discovers students' names and SSNs were inadvertently exposed on a school Web site for nearly four months.	
10/12/05	Vermont Technical College, Randolph Center, Vt.	1,100
	– Discloses that all students' names, addresses, SSNs and other info was accidentally posted on the Internet for more than a year.	
10/16/05	Georgia Tech Office of Enrollment Services	13,000
	– Reports burglary that included the theft of a computer containing names, addresses, birthdates and SSNs of current, former and prospective students.	
10/19/05	Monmouth University, West Long Beach, N.J.	667
	– Discloses that students' names and SSNs had been accidentally posted on a Web server accessible via the Internet for more than four months.	
10/21/05	TransUnion LLC	3,623
	– Distributes letters to consumers whose SSNs and other personal information contained on a desktop computer stolen in a burglary in California.	
10/21/05	University of Tennessee Medical Center, Knoxville	3,800
	– Announces the August theft of a laptop computer containing names, SSNs and birthdates of people treated at the hospital in 2003.	
10/26/05	University of Virginia	2,600
	– Discloses that names and SSNs of students and contractors of the University Housing Division were accidentally accessible via the Internet.	
11/03/05	Oregon Driver and Motor Vehicle Services	"Thousands"
	– During a drug bust, police discover a stolen laptop containing what state calls "outdated" DMV files, including names, addresses, birthdates, SSNs, etc.	

11/04/05	Ohio State University Medical Center	2,800
	– Announces that patients’ names, addresses, birthdates, phone numbers and SSNs had been mistakenly posted online for an unknown period of time.	
11/06/05	Illinois Department of Human Services	208
	– Newspaper reports it found names, addresses, birthdates and SSNs on food stamp applications that were improperly discarded at Belleville office.	
11/09/05	Firsttrust Bank, Philadelphia	N/A
	– Man pretending to be with a cleaning crew is suspected of stealing a laptop computer containing account information for thousands of bank customers.	
11/11/05	Scottrade / Troy Group	140,000
	– Notifies customers that names, SSNs, bank account numbers, other info was exposed in hacking of eCheck Secure service reported on 10/25.	
11/11/05	University of Southern California - Keck School of Medicine	50,000
	– L.A. TV station reports theft of computer server exposed names, SSNs and other personal information of employees, donors and patients.	
11/11/05	Indiana University - Kelley School of Business	5,300
	– Sends letter to students whose personal information was exposed in a computer hacking some time between August and early October.	
11/14/05	University of San Diego	7,800
	– Discovers illegal access of computer server that exposed names, addresses, SSNs and personal income tax data of faculty, students and vendors.	
11/15/05	City of Fernandina Beach, Fla.	267
	– Discloses that City Clerk accidentally e-mailed the Social Security numbers of all city employees in response to a public records request.	
11/18/05	Boeing Co.	161,000
	– Confirms theft of a laptop computer containing names, SSNs and other personal information of current and former employees.	
11/21/05	LaSalle Bank / ABN Amro Mortgage Group *	N/A
	– Discovers missing computer tape containing personal data of two million residential mortgage customers; reports on 12/10 it found the missing tape.	
11/23/05	Washington Employment Security Department	530
	– Reports theft of a laptop computer containing names, SSNs and payroll information of employees of 49 Seattle area companies.	
11/23/05	University of Delaware	952
	– Confirms two separate computer breaches in August exposed names, SSNs and other personal information of students, faculty members and others.	

12/01/05	J. Sargeant Reynolds Community College (Richmond, Va.) 26,000 – Notifies students that their names, addresses and SSNs were “inadvertently” posted on the college’s Web site for months.	
12/06/05	SAM’S CLUB 600 – Announces credit card fraud affecting cardholders who purchased gas at SAM’S CLUB stations between Sept. 21 and Oct. 2, 2005.	
12/07/05	Guidance Software 3,800 – Discovers hacking of company database in November compromised financial, personal data of customers, including law enforcement officials.	
12/07/05	Idaho State University (Pocatello) 100 – Discovers “illicit hacking program” on computer servers, exposing names, SSNs and other personal data of all students, faculty and staff for the last 10 years.	
12/09/05	Oregon Community Credit Union (Eugene) 200 – Discloses theft of an employee’s car containing insurance forms that included employee names, SSNs and other personal data.	
12/14/05	University of Dayton (Ohio) 74 – Discloses a programming error exposed on Internet the names, SSNs and other personal data of applicants to university’s pre-med program.	
12/16/05	San Joaquin County (Calif.) Human Services Agency Unknown/Not disclosed – Discloses investigation into the discovery in a dumpster of thousands of pages of documents containing clients’ names, addresses and SSNs.	
12/16/05	University of Pittsburgh Medical Center 700 – Six computers stolen from a medical office, compromising names, SSNs and dates of birth of patients.	
12/21/05	Ford Motor Co. 70,000 – Informs active and former white-collar employees of theft of computer containing company data including their Social Security numbers.	
12/22/05	H&R Block Unknown/Not disclosed – Begins notifications that it had accidentally exposed their Social Security numbers on mailing labels of free copies of its tax return software it had mailed to customers.	
12/24/05	Iowa State University 5,500 – Confirms hacking of two computers; one containing credit card info of athletic department donors; the other held SSNs of university employees.	
12/25/05	BancorpSouth 6,500 – Announces deactivation of MasterMoney debit cards because “account numbers were either lost or they were somehow hacked into” via an unnamed merchant.	

- 12/25/05 **People First / Convergys** Unknown/Not disclosed
 - Tallahassee Democrat reports personal information of tens of thousands of Florida state employees was exposed due to defects in personnel data-scanning program.

- 12/27/05 **University of Kansas** 9,200
 - Shuts down Web site that potentially exposed names, addresses, dates of birth, credit card numbers, SSNs of applicants for university housing.

- 12/27/05 **Marriott International**..... 206,000
 - Discloses missing computer tape containing credit card account info, SSNs of time-share owners and customers, as well as company employees.

* * *

TOTAL: 152 disclosed incidents, potentially affecting more than 57.7 million individuals

* *'Incidents' with asterisk (Westlaw, I.R.S., Blue Cross Blue Shield of North Carolina and Blue Cross Blue Shield of Florida, LaSalle Bank / ABN Amro Mortgage Group) have been listed but not counted in the above total. While concerns have been raised about their potential for exposure of sensitive, personally identifiable information, no actionable incident has been documented or disclosed.*