

2005 Disclosures of U.S. Data Incidents

(At least 158 incidents have been disclosed, potentially affecting more than 64.8 million individuals, plus 20 unknown victim populations. Numbers not released by company with the exposure.

<u>Date</u>	<u>Entity</u>	<u>Affected</u>
1/3/05	George Mason University <ul style="list-style-type: none"> Officials discover that hackers had accessed private information and Social Security numbers on students and staff. Discovered by Curtis McNay doing daily maintenance check. One computer penetrated; looked for backdoor to other GMU servers according to Joy R. Hughes, GMU chief Info officer. (<i>Washington Post</i>, Jan 13, 2005) 	30,000
1/6/05	University of Kansas <ul style="list-style-type: none"> 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 computer file with names, addresses, birthdates, phone numbers, SSN and credit card numbers was found accessible to the public on Dec. 16. "The lack of security affected students who applied and paid an application fee online between April 29, 2001 and Dec. 16, 2005," according to a University Relations news release. (<i>Kansan.com</i>, Jan 20, 2006) 	1,400
1/05	Christus St. Joseph Hospital, Houston Texas <ul style="list-style-type: none"> 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. Official said the stolen computer may contain medical records and SSN of hundreds of its patients. "Hospital spokesperson India Hancock said the data on the computer represents less than 1% of all patient records."(<i>USA Today and the Houston Chronicle</i>, 4/26/05) 	16,000
1/05	Kaiser Permanente <ul style="list-style-type: none"> 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. (<i>The Inquirer</i>, March 14, 2005) 	140
1/18/05	University of California at San Diego <ul style="list-style-type: none"> Officials reveal a mid-November breach may have compromised names and SSNs of students and alumni. It is the third such incident at UCSD in the past year. University spokesperson Delores Davies said, "An investigation showed the hacker was using the servers to store music and movies." (<i>San Diego Union Tribune</i>, Jan. 18, 2005) 	3,500
1/20/05	University of Northern Colorado <ul style="list-style-type: none"> University officials 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. (<i>Greeley Tribune</i>, Jan 21, 2005 said 15,000, <i>Associated Press- updated story</i> 30,000 Jan 22, 2005- source: msnbc.msn.com/id/685779) 	30,000



- 1/25/05 **Science Applications International (SAIC)** Unknown/Not disclosed
- Desktop computers were stolen from the offices of SAIC, a research and engineering company, compromising personal information of current and past stockholders. “The San Diego defense contractor said the computers contained personal information on current and former stockholder.” SAIC is an employee-owned company. 45,000 may be affected. (*10 News- ABC , Jan . 28, 2005, Washingtonpost.com 12/12/05*)
- 1/26/05 **GMAC Financial Services** 200,000
- 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. (*Information Week- May 3, 2004 /2005? and Network World- 2/21/05*)
- 1/27/05 **Purdue University** 1,200
- 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. (*Lafayette (IN) Journal and Courier, 3/25/05*)
- Winter/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. Letters were sent out on March 23 to those affected by the breach. (*San Francisco Chronicle, 4/6/05*)
- 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. (*Information Week*)
- 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. (*Greensboro News and Record- Newsbank, 5/25/05*)
- 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. (*Baltimore Sun, 3/4/05;*)
- 2/20/05 **T-Mobile** 400-500
- Mobile phone accounts of Paris Hilton and 400 T-Mobile customers compromised by hackers. Update- A Massachusetts juvenile pleaded guilty to the hacking. (*Computer World, 2/21/05*)
- 2/23/05 **PayMaxx** 25,000- 100,000
- 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. (*Boston.com Business, Feb 25, 2005*)



- 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. (*Consumeraffairs.com, 2/25/05*)
- 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. The breach also included data on about 1/3 of the Pentagon staff. Sen. Charles Schumer, a New York Democrat, said he had been informed by the Senate Rules Committee that the tapes were likely stolen off a commercial plane by baggage handlers. (*Reuters, 2/26/05*)
- 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. (*Assoc. Press 4/18/05*) <http://www.dswshoe.com/pressRelease.jsp>
- 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. (*San Francisco Chronicle, David Lazarus, 4/9/05*)
- 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. (*Las Vegas Review-Journal 6/3/05*)
- 3/8/05 **Harvard University** 200
- Intruder gains access to admission systems at Harvard, Stanford and other top business schools and helped applicants log on to learn whether they had been accepted weeks before they were to find out. “Dozens of business schools (list of some schools) were affected by the breach, with their web sites vulnerable for roughly nine hours before the problem was fixed.” (*Associated Press, March 3, 2005*) Update- it appears an online news source gave instructions on how to access the info. See Northwestern University listing
- 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. (*Msnbc.com; Palm Beach Post 4/15/05*)
- 3/11/05 **Boston College** 120,000
- Announced that hackers had accessed personal information of alumni in a computer system used for fund-raising. It also appeared that the hacker had planted a program that would enable him to launch attacks on other machines. (*Boston Globe, 3/17/05*)



- 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. (*ABC World News Tonight, 4/14/05; Washington Post 3/28/05*) Update- it was found but the info was erased.
- 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. (*Columbus Dispatch 4/16/05*)
- 3/18/05 **University of Nevada, Las Vegas** 5,000
- Administrators reveal that a hacker had been accessing the personal information of international students. The breach was discovered during a routine security check on network systems. (*Las Vegas Review Journal, 3/19/05*)
- 3/23/05 **Mutual funds** Unknown/Not disclosed
- *Wall Street Journal* 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. (*Wall St. Journal*)
- 3/25/05 **Northwestern University** 17,500-21,000
- Hackers broke into a graduate school server, exposing the Social Security numbers of students, faculty, and alumni. The Kellogg School of Management is just one of about a dozen business school that were exposed due to an article in BusinessWeek's online forum with instructions on how to hack into and view confidential online admissions info at various top MBA programs. (*BusinessWeekonline, 4/12/05 Information Management Journal, 7/05*)
- 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. A former branch manager at a San Jose medical group has been charged with stealing the confidential records of nearly 185,000 patients -- mostly South Bay residents, authorities reported. The San Jose incident is one of the nation's largest cases of personal data theft. , The U.S. attorney's office charged Joseph Nathaniel Harris on Friday with stealing two computers and a compact disc that contained patient records from the San Jose Medical Group on March 28, according to a complaint filed in U.S. District Court in San Jose. (*San Francisco Chronicle, May 15, 2005; Fortune 5/16/05*)
- 3/28/05 **University of Chicago Hospital** 85
- Announced an employee had been selling patient records. The FBI believes it could involve dozens of patients. UC officials say as many as 85 patients may have been affected. (*ABC7 Chicago, 2/18/05*)
- 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. The breach is the second this year at ISU. In March, officials discovered that the Social Security numbers of nearly 100 ISU students had been accessible to the public for more than three years on the university's Web site. Officials at Idaho State University say identity theft is unlikely, even though an illicit hacking program was discovered to have accessed personal records of all the school's students, faculty and staff for the last 10 years. Randy Gaines, ISU's chief information officer, said the hacker who launched the program



is probably from another country and not aware the personal information had been accessed. (Assoc Press, 12/9/05)

- 4/05 **MCI**..... 16,500
 - Long-distance phone company acknowledges the theft in April of a laptop computer from a car that was parked in the garage at the home of an MCI financial analyst that contained names and SSNs of current and former employees. They declined to say if the employee was authorized to carry such information on a laptop. (*Wall St. Journal*, 5/23/05)

- 4/5/05 **University of California, Davis**.....1,100
 - The names and Social Security numbers of about 1,100 students, faculty, visiting speakers and staff may have been compromised by a hacking into a main computer in the university's plant biology section last month. (*Davisenterprise.com*, 4/5/05)

- 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. Chesley Moroz, Eastern's president, says the breach affected no more than 15,000 because that is all who are in the database for the past six years." (*Philadelphia Inquirer* 4/18/05;

- 4/10/05 **Carnegie Mellon University, Pittsburgh** 5,000-6,000
 - 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. The affected computers had information for people who got graduate degrees from the Tepper School of Business between 1997 and 2004. (*MSNBC, Assoc. Press*, 4/21/05)

- 4/12/05 **Tufts University** 106,000
 - Begins notifying 106,000 alumni about "abnormal activity" on a computer used for fundraising that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers. (*Columbus Dispatch* 4/16/05; *Money Magazine* 6/7/05; *Boston Globe* 4/12/05)

- 4/13/05 **Polo Ralph Lauren / HSBC North America** 180,000
 - Credit card issuer begins notifying consumers (who used General Motors-branded MasterCard to make purchases at Polo Ralph Lauren) that criminals may have obtained access to their credit-card information. (*ABC World News Tonight* 4/14/05)

- 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. (*Sacramento Bee*, 5/28/05)

- 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. The IRS fixed 32 of the 53 problems found in a 2002 review, the GAO said, but it found 39 new security problems on top of the 21 that remain unfixed. (*Reuters* 4/18/05)
<http://www.gao.gov/new.items/d05482.pdf#search=%22internal%20revenue%20service%20gao%22>



- 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. The company realized the tap was missing in February when it was damaged during shipping. It involved customers from 2000-2003, according to spokeswoman Donna Kush. (*Assoc. Press 4/19/05*)
- 4/23/05 **Georgia Southern University, Statesboro, Ga.**Potential for “Thousands”
- Hackers broke into a GSU server that contained thousands of credit card and Social Security numbers. Affected is anyone who made a purchase at the university bookstores between Jan. 1, 2002- April 26, 2005. Also affected were those who make purchases at the campus and stadium locations, as well as on the Web site or those who received bookstore credit through their scholarship or financial aid between fall 2003 and spring 2005. (*Assoc. Press 4/28/05*)
- 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 was made public via media reports on May 5. <http://www.whartoncenter.com/FAQ/default.htm>
- 4/26/05 **Foster Wheeler, Clinton, N.J.** 6,700
- Engineering/construction company writes in May 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. (*The Morning Call, Allentown, PA., 5/7/05*)
- 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. Roughly 10 banks may have been compromised over a four-year period, according to police in Hackensack, NJ. (*Wall St Journal, 5/23/05; Money.cnn.com 5/23/05*)
- 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. (*Associated Press, 10/21/05*)
- 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 enrollments). The laptop from the career services office contains Social Security numbers and other personal information about students. (*Tulsa World, 4/30/05*)
- 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. According to the Register the hacker had access to the user name and password for 165 computers at the University. (*The Register, 4/29/05*)
- 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. A cooler-sized container of tapes apparently was lost during a truck ride. Information dated back to 1986. (*Wall St. Journal 5/3/05; CNN 5/2/05*)



- 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. (*The Denver Channel.com/7, 5/2/05*)
- 5/5/05 **Purdue University**..... 11,360
- Computers breached over a 17-day period, compromising personal information of current and former employees. Over the past year, CNET has reported security breaches at Notre Dame, Purdue, and Georgetown universities. Purdue reports third computer security breach in past years. (*Assoc. Press 5/20/05; Indianapolis Star, 5/21/05*)
- 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, driver's license numbers and history, and SSNs, including Boston Mayor Menino and Mass. Gov. Romney. (*Insurance Information Institute Database 5/5/05; Boston Globe 5/5/05*)
- 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. (*Washington Post, 6/1/05*)
- 5/11/05 **Stanford University** 10,000
- University confirms breach of computer network, stealing SSNs and other personal information of recruiters and students. The intrusion occurred at the Career Development Center on May 11th, according to Stanford general counsel Debra Zumwalt. (*CNET News, 5/25/05*)
- 5/12/05 **Merlin Information Services** 9,000
- Kalispell, Mont. This data company acknowledges names, addresses, SSNs were compromised in fraudulent access incident(s) in March/April. There appears a number of victims from this breach. The company provides info to investigators, collection agencies, insurance companies and governmental entities plus to people looking for lost loved ones, assets and running background checks (*Daily Inter Lake, 5/13/05*)
- 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. (*Chicago Sun Times, 5/13/05*)
- 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, according to Bank President Joseph MacDonough. (*Assoc Press, Boston.com, 5/19/05*)
- 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. Those at risk are all students since 1997, current employees and those who left between 1997-1999. (*Associated Press 5/21/05*)
- 5/18/05 **Jackson (Mich.) Community College** 8,000
- University press release confirms breach of computer system, potentially compromising employee and student SSNs. (*Government Technology; AP 5/23/05*)



- 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. Victims have reported use of the compromised credit card numbers Includes update. (*emailbattles.com, 5/18/05*)
- 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. (*Daily Utah Chronicle, 7/5/05*)
- 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, alumni and others. (*Raleigh News & Observer, 6/5/05*)
- 5/27/05 **Cleveland State University** 44,000
- University confirms theft of a laptop computer from its admissions office, compromising students' addresses and SSNs. (*AP 6/3/05*)
www.csuohio.edu/news/releases/2005/06/13617.html
- 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. The thief broke into the Chicago office over Memorial Day weekend. Police are investigating. (*Reuters, 6/10/05*)
- 6/2/05 **Jackson High School, Jackson Township, Ohio** Unknown/Not disclosed
- At least three students have been charged with illegally accessing school computers to change grades and acquire teachers' SSNs, credit card information and addresses. (*Akron Beacon Journal, 6/ 30/05; Canton Repository 5/27/05*)
- 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. Professor charged with stealing students' identities. Each class, Slosberg had asked his students to write their names and Social Security numbers on a sign-in sheet. Another student, Amanda Bracewell, Told The Tampa Tribune, "We all signed it,.. We figured he's a teacher, what is he going to do with it?" (*The Associated Press, 6/6/05; Tampa Tribune 2005*)
- 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. "We deeply regret this incident, which occurred in spite of enhanced security procedures we require of our couriers," said Kevin Kessinger, Exec VP of Citigroup's Global Consumer Group. (*Bloomberg News, June 6, 2005; AP June 6, 2005*)
- 6/10/05 **Federal Deposit Insurance Corp. (FDIC)** 6,000
- On June 10, 2005 begins notifying current and former employees of a 2004 breach that may have compromised their names, SSNs, DOBs, salaries and employment information. The letter states that it included data on all FDIC employees that were in an official pay status since July 2002. (*Washington Post; GovExec.com, 6/17/05*)



- 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. (*Cleveland Plain Dealer*, 6/18/05)
- 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 on all 10 campuses. (*The Hawaiichannel.com*, 6/17/05))
- 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. (*NY Times*; *msnbc.com*, 7/19/05)
- 6/22/05 **Eastman Kodak**..... 5,800
- Confirms it has begun notifying former employees that their names, SSNs, birthdates and other information was on a password-protected laptop computer stolen from a consultant's car. Kodak is in the process of sending out letter to employees from the last 3 years. (*Democrat & Chronicle*, 6/22/05)
- 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 for the physician assistant studies program. Computer specialists discovered the breach in May while repairing the server after complaints of slow computer speed. (*University Wire*, 7-19-05; *Daily Reflector*, 6-22-05)
- 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. (*AP* 6/24/05; *CNET News*, 6/28/05)
- 6/27/05 **Michigan State University, Human Resources Dept.**..... undisclosed
- Media reports on 7/7 reveal a breach within the human resources department that may have exposed SSNs of all university employees and retirees. (*State News*, 7/7/05)
- 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. Lt. Machura of the Toledo Police Dept. says an agency employee is the prime suspect. (*The Blade*, Toledo, OH, 6/28/05)
- 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. Authorities notified department officials of the breach in early April. In at least five cases so far, the information has been used. (*Richmond Times-Dispatch*, 6/29/05)
- 6/30/05 **Ohio State University Medical Center** 15,000
- Confirms notifications to patients whose names and billing information was contained. A laptop stolen from an Indianola Avenue consultant's office in April held names and billing information for about 15,000 Ohio State University Medical Center patients. Hospital officials investigated the theft after MTE Consulting notified them in late April. (*Columbus Dispatch* 6/30/05)



- 7/1/05 **University of California at San Diego** 3,300
- Confirms fourth hacking since April 2004. SSNs, driver's license, credit card numbers of students, staff and faculty were compromised in incident in April. (*San Diego Union Tribune, 7/1/05*)
- 7/1/05 **Blue Cross and Blue Shield of North Carolina *** Unknown
- The health insurer accuses ProCare of conspiring with one or more Blue Cross employees to obtain internal documents. Information was posted on the www.procare.org website. (This incident is not currently included in our list, pending more clarification) (*Charlotte Observer, 7/2/05*)
- 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 Apparently Iron Mountain lost track of the tapes. Melissa Burman, an Iron Mountain spokeswoman, told Lazarus that there had been four events of human error since the beginning of the year. (*San Francisco Chronicle, David Lazarus, 7/6/2005; Los Angeles Times 7/6/05*)
- 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. (*State News, East Lansing, 7/7/05*)
- 7/8/05 **University of Southern California** 270,000
- Confirms a hacker (since 1997) may have gained access to students' names, Officials at USC said they will contact everyone who use3d the school's online application program in the past 8 years after learning about a security flax that allowed people to view past forms. (*Associated Press- 7/11/05*)
- 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 "They also contained partial health treatment histories for some patients and some information about the doctor who provided the care," said Biodyne spokeswoman Erin Somers. (*AP 7/13/05; Arizona Republic*)
- 7/14/05 **University of Colorado** 42,000
- Breach of Wardenburg Health Center computer server exposes names, SSNs, ID numbers, addresses, and birthdates of students, faculty, staff, and visitors. (*UPI Boulder, 7/22/05, University Press Release listed below*)
- 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. (*University press release- <http://www.colorado.edu/news/releases/2005/280.html>*)
- 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. (*Forbes 9/6/05*)



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. (<i>TheIowaChannel.com, 7/20/05</i>)	
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 including members of the justice and law enforcement communities. (<i>San Diego Union Tribune; North County Times 7/30/05</i>)	
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 were stolen from a microfilming company. The records included information from 2002-2004. (<i>AP, 7/25/05</i>).	
7/26/05	California State University, Dominguez Hills	9,613
	• Discovers the unauthorized access of three desktop computers containing names and SSNs of 3/4 th of its student applicant records. (<i>AP, 7/29/05</i>)	
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, and staff. (<i>Denver Post 8/3/05</i>)	
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. (<i>Leaf Chronicle, Clarksville TN 7/30/05</i>) See note 8/10	
7/29/05	Cal Poly Pomona	31,077
	• Interim VP of instructional and information technology Debra Brum confirms a 6/29 hacking of two computer servers, compromising names and SSNs of current and former faculty, staff, students and university applicants. (<i>Whittierdailynews.com, 8/4/05</i>) See college news release- http://www.csupomona.edu/%7Enews/releases/pdf/R0506-003.pdf	
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. (<i>WYFF4.com, 8/4/05</i>)	
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. (<i>San Francisco Chronicle/sfgate, 8/9/05</i>)	
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. (<i>Dallas News, dallasnews.com, 8/9/05</i>)	



- 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. (*The Blade*, 8/17/05)

- 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. A JP Morgan spokeswoman would not say how many accounts were affected. (*Forbes*, 8/30/05)

- 8/9/05 **University of Utah**..... 100,000
 - Confirms notification due to apparent “hacking” of a computer server containing names and SSNs of former employees, 1970 to 2003. (*ABC4*, 8/10/05; *univ. PR-www.utah.edu/unews/releases/05/august/server.html*)

- 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. The CD disappeared early last month when a company was sending it back to Iowa Student Loan via private courier. The package was found empty according to Steve McCullough, Iowa Student Loan chief executive. (*Associated Press*, 9/1/05)

- 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 more than a month prior. (*Greeley Tribune*).

- 8/10/05 **Austin Peay State University, Clarksville, Tenn.**..... 1,280- 1,500
 - School confirms additional exposure of students’, vendors’ names, SSNs, addresses, phone numbers, and other info due to problem with school’s Web site. (*NewsChannel5*, 7/5/05)

- 8/10/05 **California State University, Stanislaus** 877
 - Discovers a breach of a computer file server containing names, SSNs of student workers. Maithreyi Manoharan said the university was investigating the case internally and had not contacted law enforcement officials. (*Modesto Bee*, 8/16/05)

- 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 at Randolph Air Force Base in Texas. The unusually high activity on the account was noted in June. (*Washington Post*, 8/22/05; *Government Computer News* 8/19/05)

- 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 dating from June 1999 to May 2001 and from fall 2003 to summer 2005 could have been accessed, the university said. (*Assoc. Press*, 8/19/05)

- 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. (*Gainesville Sun*, 8/27/05)



- 8/20-21/05 **U.S. Army, Fort Carson, Colo.** 15,000
 - Confirms on Sept. 12 the theft of four computer hard drives in the Soldier Readiness Processing Center containing names, SSNs and personal records of soldiers processed at Fort Carson. (*rockymountainnews.com, 9/13/05*)

- 8/21-22/05 **Kent State University** 100,000
 - Confirms on Sept. 9 the theft of 5 computers containing the names and SSNs of current and former students and professors. The information goes back to 2000 for students and faculty and 2002 for instructors. (*Plain Dealer Reporter, 9/10/05*)

- 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. “The college learned of the problem Monday morning through emails sent by students,” said Irene Motts, director of marketing and communications at Stark State. (*CantonRep.com, August 30, 2005*)

- 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. (*Bay City News via KPIX-TV San Francisco, 8/29/05*)

- 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. Two years ago, Blue Cross voluntarily began to do away with Social Security-based policy numbers. The old IDs, however, were not updated for one group of customers. In addition, the policy number field that should have been omitted from the label was still present, said Randy Kammer, the company’s vice president of regulatory affairs and public policy. (*The Florida Times Union, 9/1/05*)

- 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. (*Union Tribune; AP, 9/19/05*)

- 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. Affected students were enrolled on all campuses in the fall of 2002. (*AP; Dayton Daily News, 9/16/05*)

- 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). (*Newsday, 9/17/05*)

- 9/19/05 **University of Georgia** 1,600- 2,429
 - Discovers unauthorized computers access, believed to be from another country, which exposed names, SSNs of current and former employees. But the breach also affects others who have received payments from the College, said Tom Jackson, a UGA spokesman. No credit card information was exposed, Jackson said. University officials say 2,429 Social Security numbers were exposed, but there was some repetition and the number of affected people is expected to be smaller. Last year, a hacker broke into a UGA computer and may have accessed credit card information for about 32,000 students. The university never caught the hacker, but it also is not aware of any misuse of that information, Jackson said. (*Associated Press, 9/28/05*)



9/21/05 City College of New York	9,000
<ul style="list-style-type: none">• Acknowledges that CUNY Law School employee and students' names, SSNs and other personal info were accidentally posted on a university Web site. It is more widespread than first reported. CUNY officials detected the unprotected payroll link for the Hunter College Campus Schools last week. (newsday.com, 9/28/05)	
9/22/05 ChoicePoint	5,000
<ul style="list-style-type: none">• Makes notifications stemming from misuse of IDs/passwords by customers, including a police department, insurance company, P.I. firm and others. http://www.msnbc.msn.com/id/9370909/	
9/22/05 World Trade Center Medical Monitoring Program	10,000
<ul style="list-style-type: none">• 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. Bronx man arrested according to the police for the crime. (<i>Star Ledger</i> 10/1/05; <i>NY Times.com</i> Sept. 29, 2005)	
9/23/05 Bank of America	Unknown/Undisclosed
<ul style="list-style-type: none">• Sends letters re: 8/29 theft of laptop computer containing Visa Buxx users' names, account numbers, routing transit numbers and credit card numbers. The letters, dated Sept. 23, only said the computer was "stolen from one of our service providers that had been managing on our behalf." Visa Buxx are prepaid debit cards parents can use to provide money to teens. (<i>San Francisco Chronicle</i>, 10/7/05)	
9/27/05 RBC Dain Rauscher	100
<ul style="list-style-type: none">• Notifies customers of illegal access to customer data by former employee who wrote anonymous letters saying he/she had compromised data. The brokerage manages some 300,000 accounts. (<i>Associated Press</i> 9/27/05)	
10/05/05 Wilcox Memorial Hospital, Kauai, Hawaii	130,000
<ul style="list-style-type: none">• Discloses on 10/17 the theft of a back-up computer hard drive (flash drive) containing patients' names, addresses, SSNs and medical record numbers, according to Lani Yukimura, marketing director. (<i>The Garden Island</i>, 10/20/05)	
10/07/05 Montclair State University, Montclair, N.J.	9,100
<ul style="list-style-type: none">• Discovers students' names and SSNs were inadvertently exposed on a school Web site for nearly four months. All 16,000 students were informed of the problem, though only the files of the undergraduates who had declared a major and had been assigned an advisor were on the web. (<i>Star Ledger</i>, 10/15/05)	
10/12/05 Vermont Technical College, Randolph Center, Vt.	1,100
<ul style="list-style-type: none">• Discloses that all students' names, addresses, SSNs and other info were accidentally posted on the Internet for more than a year. (<i>AP</i>, 10/20/05)	
10/16/05 Georgia Tech Office of Enrollment Services	13,000
<ul style="list-style-type: none">• Reports burglary that included the theft of a computer containing names, addresses, birthdates and SSNs of current, former and prospective students. (<i>University Wire</i>)	
10/19/05 Monmouth University, West Long Beach, N.J.	667
<ul style="list-style-type: none">• Discloses that students' names and SSNs had been accidentally posted on a Web server accessible via the Internet for more than four months. (<i>Star Ledger</i>, 10/20/05)	



10/21/05	TransUnion LLC	3,623
	<ul style="list-style-type: none">Distributes letters to consumers whose SSNs and other personal information contained on a desktop computer stolen in a burglary in California. (<i>Washington Post</i>, 11/9/05)	
10/21/05	University of Tennessee Medical Center, Knoxville	3,800+ 1,900
	<ul style="list-style-type: none">Announces the August theft of a laptop computer from the billing office containing names, SSNs and birthdates of people treated at the hospital in 2003. The hard drive was stolen on Aug. 25 but letters were not mailed out until Oct 21. (<i>Knoxville News Sentinel</i>, 11/1/05; <i>Assoc Press</i> 11/1/05) Note- additional breach of 1,900 on 10/29- (<i>Tennessean.com</i>)	
10/26/05	University of Virginia	2,600
	<ul style="list-style-type: none">Discloses that names and SSNs of students and contractors of the University Housing Division were accidentally accessible via the Internet. The information was stored on a public website. (<i>Cavalier Daily-University of Virginia</i>, 10/31/05)	
10/29/05	University of Tennessee	1,900
	<ul style="list-style-type: none">The school notified students and employees yesterday that their names and SSNs were inadvertently posted on the Internet. A student made the discovery about 2 weeks prior to the notification. (<i>The Tennessean</i> 10/29/05)	
11/03/05	Oregon Driver and Motor Vehicle Services	"Thousands"
	<ul style="list-style-type: none">During a drug bust, police discover a stolen laptop containing what state calls "outdated" DMV files, including names, addresses, birthdates, SSNs, etc. (<i>The Oregonian, Portland</i>, 11/5/05)	
11/04/05	Ohio State University Medical Center	2,800
	<ul style="list-style-type: none">Announces that patients' names, addresses, birthdates, phone numbers and SSNs had been mistakenly posted online for an unknown period of time. One article said it only had affected those who made or changed appointments on April 19, 2004. (<i>Columbus Dispatch</i>, 11/4/05)	
11/5/06	Safeway, Hawaii	1,400
	<ul style="list-style-type: none">Employees' names, SSN and other personal info was stolen from a manager's laptop in California. "Our members received notification two months after the original incident...", "said Pat Loo of the United Food and Commercial Workers Union. The theft was in August. (<i>KHON</i>, 11/5/05)	
11/06/05	Illinois Department of Human Services	208
	<ul style="list-style-type: none">Newspaper reports it found names, addresses, birthdates and SSNs on food stamp applications that were improperly discarded at Belleville office. (<i>Belleville News-Democrat.com</i>, 11/6/05)	
11/09/05	Firsttrust Bank, Philadelphia	N/A
	<ul style="list-style-type: none">Man pretending to be with a cleaning crew is suspected of stealing a laptop computer containing account information for thousands of bank customers. (<i>Northeasttimes.com</i>, 12/8/05)	
11/11/05	Scottrade / Troy Group	140,000
	<ul style="list-style-type: none">Notifies customers that names, SSNs, bank account numbers, other info was exposed in hacking of eCheck Secure service reported on 10/25. The service was provided through a third party, Troy Group Inc. (<i>St. Louis Post-Dispatch</i>, 11/29/05)	



- 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. (*KNBC-TV, MSNBC, 11/4/05*)
- 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. (*Assoc Press, 11/17/05*)
- 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. (*San Diego Union Tribune, 12/3/05*)
- 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. (*The Florida Times-Union, Jacksonville, FL 11/19/05*)
- 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. (*MSNBC; Reuters, 11/18/05*)
- 11/21/05 **LaSalle Bank / ABN Amro Mortgage Group *** 2 million
- Discovers missing computer tape containing personal data of two million residential mortgage customers; reports on 12/10 it found the missing tape. It had been lost in transit and contained names, account info, payment histories and SSN. (*Reuters News, 12/16/05*)
- 11/23/05 **Washington Employment Security Department**..... 800
- Reports theft of a laptop computer containing names, SSNs and payroll information of employees of 49 Seattle area companies between January 2002 and October 2005. (*fortress.wa.gov, 12/6/05*)
- 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. (*The News Journal Wilmington, Del., 11/30/05*)
- 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. (*WAVY, Richmond VA, 12/9/05*)
- 12/2/05 **Cornell Information Technology (CIT)**.....900
- Employees discovered a breach containing names, addresses, SSNs, bank names and accounts numbers on about 900 individuals. The affected individuals were notified in November. Simeon Moss, Cornell’s press office director, said that those individuals who had information stored on the computer were not initially contacted when the problem was detected, because CIT wanted to make sure the security breach was analyzed properly - a time consuming and work intensive process. (*Cornell Sun.com, 12/2/05*)
- 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. Kayce Bell, chief operating officer at Alabama Credit Union (ACU) in Foley, Ala., said the company is reissuing cards to about 500 credit card and debit card



holders as a result of the breach. The credit union was alerted to the problem last week by Credit Union National Association Inc., she said. "We received information through our national reporting service that there had been a very large breach of data at Sam's Club," Bell said. About 500 debit cards and credit cards issued by ACU were among the accounts compromised in this incident, she said. (*Computerworld*, 12/12/05)

- 12/07/05 **Guidance Software**..... 3,800
 - This leading provider of software used to diagnose hacker break-ins has itself been hacked. The breach in November compromised financial, personal data of customers, including law enforcement officials. (*Washington Post*, 12/19/05) [9/AR20051190092.html](#)

- 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. (*AP*, 12/9/05)

- 12/8/05 **San Antonio Independent School District**.....1,000+
 - The elementary school teachers learned that a stolen laptop with their names, birthdates, and SSN was stolen earlier in the week. It included info on nearly all the pre-kindergarten, first, second and third grade teachers in the district. The laptop belonged to a district employee and left it in the car. (*News4WOAI*, 12/8/05)

- 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. (*Credit Union Journal*, 12/19/05)

- 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. (*Akron Beacon Journal*, 12/15/05)

- 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. The announcement came after thousands of pages of country mental health documents were found in a Stockton recycling center. The documents were used by the agency to refer clients to CalWORKS. (*The Record, Stockton*, 12/18/05)

- 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. Six computers containing 700 patients information were stolen from the Squirrel Hill Family Medicine offices, which are owned by the University of Pittsburgh Medical Center according to UPMC spokeswoman Jan Duffield. (*Assoc. Press* 1/2/06)

- 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. (*CNN Money.com*, 12/22/05)

- 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. (*CNET News*, 1/3/06)

- 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. (*Des Moines Register*, 12/12/05)



- 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. (*News 7, Laurel-Hattiesburg, MS, 12/26/05*)
- 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. (*Tallahassee Democrat, 12/25/05*)
- 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. (*Kansas City Star, 12/28/05*)
- 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. Officials at Marriott Vacation Club International said it is not clear whether the tapes were stolen or lost from the Orlando headquarters. (*Washington Post, 12/28/05*)
- March 05**State of Michigan**..... 8.2 million plus
 - State databases with confidential information from registered voters and driver’s licenses in Michigan was not adequately secure according to an audit that was just made available in March 2005. State auditors said that the system included about 7/2 driver’s licenses, 1 million personal identification cards (as of Jan 2004) and had similar concerns with the Qualified Voter File. The report covers records from Sept. 30, 1997 to June 30, 2004. The Voter file has names and addresses of about 6.8 million registered voters. (*Assoc Press, freep.com, Lansing, MI, 3/18/05*)

TOTAL: 158 disclosed incidents, potentially affecting more than 64.8 million individuals plus 20 undisclosed victim group populations.

‘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.