



Identity Theft Resource Center Reports 104 Security Breaches Since January 1st

Is Anyone Hearing An Alarm Bell Yet?

SAN DIEGO, Sept. 6 /PRNewswire/ -- Since January 1, 2005, through public announcements and media reports, at least 104 data incidents have been documented in the U.S., potentially affecting more than 56.2 million individuals. And that is probably just the tip of the iceberg.

How many breaches don't make the front page or are even reported to consumers because a company has deemed the breach to not "cause significant risk of harm" to the individual or buried it to avoid additional problems? We will never know. What we do know is that security breaches are not new - they have been occurring for years. What is different is that now you are hearing about them.

While Congressional committees wage a turf war over a security breach notification law, companies, governmental agencies and educational facilities are mishandling information on a daily basis - putting all of us at risk of identity theft.

However any notification law is only a bandage to cover a more significant problem - personal information leakage - a subject that industry would rather Congress NOT address.

Security breaches fall into a number of easily recognizable patterns:

- Lost or stolen laptops, computers or other computer storage devices without password protection
- Unprotected backup tapes lost in transit because they were not sent either electronically or with a human escort
- Hackers breaking into systems
- Employees stealing information or allowing access to information such as via call centers
- Information bought by a fake business
- Poor business practices - for example sending postcards with Social Security numbers on them or requiring students to place name and SSN on rosters that are passed through classrooms or placed on papers or tests
- Internal security failures including the inability to track personal information through the entire entity's system
- Viruses, Trojan Horses and computer security loopholes
- Information tossed into dumpsters - improper disposition of information

While it may be impossible to stop some hackers, most of these breaches could have been avoided by following safe information handling practices. Let us not forget: "Those who cannot remember the past are condemned to repeat it." George Santayana (*The Life of Reason*, Vol. 1, 1905)

Why were there 4 breaches that involved the shipment of backup tapes without adequate protection? More than half of the breaches listed were educational facilities. The University of Colorado leads the group with FOUR breaches in just this one year. Michigan State University comes in a close second with three. WHY? Why are student Social Security numbers still being used as ID numbers and put on laptops that are not even password protected?

Something has to change or we might as well give up the battle against identity theft and protecting the privacy of our information now. Congress needs to take action - not at the expense of consumers but in creating laws

and assisting companies to better control their information. Under the current legislation pending, the only time you will hear of a breach is when a company (some of the same ones that until this year did not disclose breaches) believes there is significant harm that may occur. Responsible corporate lawyers, fraud investigators, computer security specialists and members of law enforcement will tell you - no one can predict the future or how a thief might use illegally obtained information.

We have been given a loud wake-up call. Is anyone planning to pay attention to the true problem or will companies be allowed to continue to disregard the importance of your future and your financial identity?

Jay Foley and Linda Foley, the co-directors of the nonprofit Identity Theft Resource Center, are available for comment. 858-693-7935

The Identity Theft Resource Center has two programs available for companies that assist with breaches. One program is designed to help companies who have just experienced a breach. The other program is a unique assessment tool to help companies see their business "through the eyes of a thief."

2005 Disclosures of U.S. Data Breach Incidents

(At least 104 incidents have been disclosed, potentially affecting more than 56.2 million individuals)

Date	Entity	Affected
01/03/05	George Mason University	30,000
	- Officials discover that hackers had accessed private information and Social Security numbers on students and staff.	
01/06/05	University of Kansas	1,400
	- Administrators send letters to individuals whose personal information, including Social Security numbers, passport numbers, countries of origin, and birth dates, might have been compromised when a hacker accessed a server in November 2004.	
01/05	Christus St. Joseph Hospital, Houston Texas	16,000
	- 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.	
01/05	Kaiser Permanente	140
	- 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.	
01/18/05	University of California, San Diego	3,500
	- Officials reveal a mid-November breach may have compromised names and SSNs of students and alumni.	
01/20/05	University of Northern Colorado	30,000
	- 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.	
01/25/05	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.
- 01/26/05 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.
- 01/27/05 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.
- 02/05 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.
- 02/02/05 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.
- 02/10/05 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.
- 02/14/05 ChoicePoint 145,000

- Company confirms customer fraud in which public records information about approximately 30,000 consumers may have been compromised; number of potentially affected consumers later increased to 145,000.
- 02/20/05 T-Mobile 400

- Mobile phone accounts of Paris Hilton and 400 T-Mobile customers compromised by hackers.
- 02/23/05 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.
- 02/24/05 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.
- 02/25/05 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.
- 03/08/05 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.

- 03/05 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.

- 03/08/05 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.

- 03/09/05 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.

- 03/11/05 Boston College 120,000
 - Announced that hackers had accessed personal information of alumni in a computer system used for fund-raising.

- 03/11/05 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.

- 03/07/05 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.

- 03/14/05 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.

- 03/18/05 University of Nevada, Las Vegas 5,000
 - Administrators reveal that a hacker had been accessing the personal information of international students.

- 03/23/05 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.

- 03/25/05 Northwestern University 21,000
 - Hackers broke into a graduate school server, exposing the Social Security numbers of students, faculty, and alumni.

- 03/28/05 San Jose Medical Group 185,000
 - Two computers stolen containing patient billing information, including names, addresses, Social Security numbers and confidential medical information.

- 03/28/05 University of Chicago Hospital Unknown/Not disclosed

- Kalispell, Mont., data company acknowledges names, addresses, SSNs were compromised in fraudulent access incident(s) in March/April.

- 05/12/05 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.

- 05/16/05 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.

- 05/17/05 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.

- 05/18/05 Jackson (Mich.) Community College 8,000
 - University confirms breach of computer system, potentially compromising employee and student SSNs.

- 05/18/05 University of Iowa 30,000
 - University confirms breach of campus book store computer system, potentially compromising employee and student IDs and credit card numbers.

- 05/23/05 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.

- 05/26/05 Duke University Medical Center 14,000
 - School says that a hacker broke into its computer system and stole names, passwords and partial SSNs of employees, physicians and others.

- 05/27/05 Cleveland State University 44,000
 - University confirms theft of a laptop computer from its admissions office, compromising students' addresses and SSNs.

- 05/28-30/05 Motorola 30,000
 - Confirms theft of computers from HR services provider, Affiliated Computer Services, exposing its U.S. employees' personal data, including SSNs.

- 06/02/05 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.

- 06/03/05 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.

06/29/05	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.		
06/30/05	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.		
07/01/05	University of California 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.		
07/01/05	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).		
07/05/05	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.		
07/05/05	Michigan State University	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.		
07/08/05	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.		
07/08/05	Blue Cross Blue Shield of Arizona	57,000
- Confirms customers' addresses, SSNs, DOBs and phone numbers were on backup tapes stolen 6/29 from Arizona Biodyne, a managed care company.		
07/14/05	University of Colorado	42,000
- Breach of Wardenburg Health Center computer server exposes names, SSNs, ID numbers, addresses, birth dates of students, faculty, staff and visitors.		
07/14/05	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.		
07/15/05	University of Delaware	343
- Confirms the December 2004 theft of three computers, one of which contained Department of Communications students' names and SSNs.		
07/18/05	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.		

07/21/05	San Diego County Employees Retirement Association	32,000
	- Discovers unauthorized access of two computer servers containing names, SSNs, birth dates and addresses of current and former county employees.	
07/25/05	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.	
07/26/05	California State University, Dominguez Hills	9,613
	- Discovers the unauthorized access of three desktop computers containing names and SSNs of students.	
07/27/05	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.	
07/29/05	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.	
07/29/05	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.	
08/03/05	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.	
08/04/05	Pennsylvania Unified Judicial System	Unknown/Not disclosed
	- Confirms "five to 10 minute access" via a Web site compromised SSNs and other confidential information of defendants on statewide computer system.	
08/08/05	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.	
08/08/05	University of North Texas, Denton, Texas	38,607
	- Discloses "hacking" of computer system exposing names, SSNs, student IDs and phone numbers of current, former, prospective students from 1999 to 2005.	
08/08/05	Huntington National Bank, Toledo, Ohio	6,000
	- Confirms distribution of notification letters due to theft of account information, including names, SSNs, signatures and account numbers of local customers.	
08/09/05	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.	

- | | | |
|----------|---|---------|
| 08/09/05 | 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. | |
| 08/10/05 | Austin Peay State University,
Clarksville, Tenn. | 1,280 |
| | - Confirms additional exposure of students' and vendors' names, SSNs, addresses, phone numbers and other info due to problem with school's Web site. | |
| 08/10/05 | California State University, Stanislaus | 877 |
| | - Discovers a breach of a computer file server containing names and SSNs of student workers. | |
| 08/18/05 | 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. | |
| 08/19/05 | University of Colorado | 49,000 |
| | - Confirms breach of computer server used by Registrar's Office, exposing names, SSNs, addresses and phone numbers of current and former students. | |
| 08/19/05 | 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. | |
| 08/25/05 | J.P. Morgan Private Bank | Unknown |
| | - Distributes letters advising of the Aug. 8 theft of a computer from its Dallas offices containing personal and financial information about its wealthy clients. | |
| 08/28/05 | Stark State College of Technology
(Jackson Township, Ohio) | Unknown |
| | - Acknowledges software "glitch" allowed students to inadvertently view personal information of other students, including SSN, GPA and 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, and SSNs of two administrators. | |

TOTAL: 104 disclosed incidents, potentially affecting more than 56.2 million individuals
 More than 1/2 of the breaches have occurred at educational facilities.

* 'Incidents' with asterisk (Westlaw, I.R.S., Blue Cross Blue Shield of North Carolina) have been listed but not counted in the above total. While concerns have been raised about their potential for exposure of personally identifiable information, no actual incident has been documented or disclosed.

SOURCE Identity Theft Resource Center

Related links:

- <http://www.idtheftcenter.org>
-

Issuers of news releases and not PR Newswire are solely responsible for the accuracy of the content.
Terms and conditions, including restrictions on redistribution, apply.
Copyright © 1996-2006 PR Newswire Association LLC. All Rights Reserved.
A **United Business Media** company.