Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

Sign In to Your Complaint Center.

Chronology of Data Breaches
Custom Sort
Select your desired results. Then click "Go!"

Choose the type of breaches to display:

Click or unclick the boxes then select go.

☑ **Unintended disclosure (DISC)** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.

☑ **Hacking or malware (HACK)** - Electronic entry by an outside party, malware and spyware.

☑ **Payment Card Fraud (CARD)** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.

☑ **Insider (INSD)** - Someone with legitimate access intentionally breaches information - such as an employee or contractor.

☑ **Physical loss (PHYS)** - Lost, discarded or stolen non-electronic records, such as paper documents

☑ **Portable device (PORT)** - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc

☑ **Stationary device (STAT)** - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.

☑ **Unknown or other (UNKN)**

Select organization type(s):

☐ BSO - Businesses - Other
☐ BSF - Businesses - Financial and Insurance Services
☐ BSR - Businesses - Retail/Merchant
☑ EDU - Educational Institutions
☐ GOV - Government and Military
☐ MED - Healthcare - Medical Providers
☐ NGO - Nonprofit Organizations

Select year(s):

☑ 2005
☑ 2006
☑ 2007
☑ 2008
☑ 2009
☑ 2010
☑ 2011
☑ 2012
☑ 2013

[GO!]
Select features, then click GO.

New Search (/data-breach/new)

Help Guide (/data-breach-how-to)

Return to Chronology main page. (/data-breach)

Breach Subtotal

Breaches currently displayed:
Breach Types: DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN
Organization Types: EDU
Years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013
10,542,478 Records in our database from.
676 Breaches made public fitting this criteria

Save or Print a PDF of **Entire Breach List** (/sites/privacyrights.org/files/static/Chronology-of-Data-Breaches_-_Privacy-Rights-Clearinghouse.pdf) (including introductory FAQ)

(/data-breach/print) **Conduct a search** of the Chronology using its sorting features, and Save or Print a PDF (/data-breach/print) of your search results (Select filters)

*I*f you do not have access to PDF, you can print the Chronology in landscape view.

Date Made Public	Name	Entity	Type	Total Records

| February 25, 2013 | **Capella University**
Minneapolis, Minnesota | EDU | INSD | Unknown |

Capella University's official breach notice can be found here
(http://www.atg.state.vt.us/assets/files/Capella%20University%20Security%20Breach%20Notice%20to%20consumer.pdf)
: http://www.atg.state.vt.us/assets/files/Capella%20University%20Security%20Breach

%20Notice%20to%20consumer.pdf

A collection department employee sent sensitive information to a personal email account. The incident was discovered on January 28 and the employee was fired. A small group of learners may have had their names, Social Security numbers, and other information that was kept by Capella's collection department exposed.

Information Source:
Security Breach Letter

records from this breach used in our total: 0

| February 21, 2013 | **Polk County School District**
Bartow, Florida | EDU | DISC | 200 |

Students who paid tuition for education programs may have had their 1098T tax forms sent to the incorrect address. Between 150 and 200 people out of 2,000 were sent to the wrong address because a group of the tax forms were placed in envelopes without being properly separated. Some people received the forms of several people while others never got their tax forms. The district implemented a new step of sampling some of the envelopes in order to review the process before completing an entire batch.

Information Source:
Media

records from this breach used in our total: 200

| February 13, 2013 | **University of North Carolina**
Chapel Hill, North Carolina | EDU | HACK | 3,500 |

A cyber attack on two servers resulted in the exposure of employee information. The servers were at the UNC Lineberger Comprehensive Cancer Center. Employees, contractors, and visiting lecturers at the Lineberger Center may have had their Social Security numbers or passport numbers exposed. The breach was discovered in May of 2012 and notifications were sent in December of 2012. Fewer than 15 people who were subjects in research studies were also affected by the breach.

Information Source:
Media

records from this breach used in our total: 3,500

| February 1, 2013 | **Antioch Unified School District**
Antioch, California | EDU | DISC | Unknown |

A document with sensitive Worker's Compensation claim information was accidentally sent out with an email to a limited number of Antioch Unified School District employees. Social Security numbers and other information related to current and former employees that reported injuries were exposed. The incident occurred on January 18 and people who received the email were instructed to remove and destroy any saved information contain in the email. Those who received the email were also instructed to provide written verification that they had removed and destroyed the information.

Information Source:
California Attorney General

records from this breach used in our total: 0

| January 24, 2013 | **Eastern Illinois University**
Charleston, Illinois | EDU | DISC | 430 (No SSNs or financial information |

reported)

At least 65 students received information about the grade point average of 430 students during early January 2013. The breach occurred when a spreadsheet that contained the information and the E-number of 430 students was accidentally made available online.

Information Source: Databreaches.net

records from this breach used in our total: 0

| January 10, 2013 | **KTSU Texas Southern University** **Houston, Texas** | EDU | INSD | Unknown |

Texas Southern University's radio station KTSU gave a volunteer position to a person with a criminal history of credit card fraud. The volunteer was later arrested for allegedly using the radio station's donation drive to steal credit card information. The dishonest volunteer faces up to 300 counts of credit card fraud for attempting to misuse the information on donor pledge sheets.

Information Source: Databreaches.net

records from this breach used in our total: 0

| January 8, 2013 | **Morgan Road Middle School** **Hephzibah, Georgia** | EDU | PORT | Unknown |

An unencrypted flash drive was stolen from a teacher's car. It contained student Social Security numbers and other information.

Information Source: Databreaches.net

records from this breach used in our total: 0

| January 8, 2013 | **Charlotte-Mecklenburg Schools** **Charlotte, North Carolina** | EDU | PHYS | 80 |

An employee working in human resources was robbed while transporting information between school districts. The employee stopped for lunch and discovered that personnel files containing names, Social Security numbers, addresses, dates of birth, and driver's license numbers had been stolen from their car.

Information Source: Databreaches.net

records from this breach used in our total: 80

| December 21, 2012 | **Fairfax High School** **Fairfax, Virginia** | EDU | HACK | Unknown |

Fairfax County Public Schools discovered that student names, ID numbers, grades, and other information were posted online. Students enrolled in 9th, 10th, and 11th grade were affected. The information may have only been available for a day before Fairfax County Public Schools began the process of removing it from online.

Information Source: Databreaches.net

records from this breach used in our total: 0

| December 18, 2012 | **Western University of Health Sciences** **Pomona, California** | EDU | DISC | Unknown |

Western University of Health Sciences' BanWeb Self-Service Federal Work Study reports were accessible to people who used BanWeb with a Western University of Health Sciences user ID and password. The reports contained names, Social Security numbers, and direct deposit bank account information in some cases. The information was available for an unspecified amount of time. Western University of Health Sciences conducted an investigation and reported that there was no reason to believe sensitive information was accessed by unauthorized BanWeb users. Western University of Health Sciences disabled access to the reports after learning about the breach on

November 14. Notifications were sent on December 18.

Information Source:
California
Attorney General

records from this breach used in our total: 0

| December 12, 2012 | **Mt. Diablo Unified School District** **Concord, California** | EDU | STAT | Unknown |

A December 1 office burglary resulted in the theft of an unencrypted computer. The computer contained files that included current and former Mt. Diablo Unified School District employee names, Social Security numbers, dates of birth, and addresses. People who were employees between 1998 and 2010 may have been affected.

Information Source:
California
Attorney General

records from this breach used in our total: 0

| December 11, 2012 | **Pepperdine University** **Malibu, California** | EDU | PORT | 8,300 |

A University laptop was stolen from an employee's locked car. Pepperdine learned of the theft on November 12, 2012. The laptop may have contained names, Social Security numbers, addresses, and/or dates of birth.

UPDATE (12/11/2012): As many as 8,300 people may have been affected. The laptop had been used for work related to the IRS and contained data from as far back as 2008. About 75 percent of the people affected were students.

Information Source:
California
Attorney General

records from this breach used in our total: 8,300

| November 22, 2012 | **Scripps College** **Anaheim, California** | EDU | PHYS | 940 (No SSNs or financial information reported) |

Scripps College is located in Claremont, California and the theft took place in Anaheim, California.

Sensitive records were stolen from a tote bag in a staff member's vehicle on the night of November 18. The records included names, dates of birth, cell phone numbers, email addresses, and emergency contact information.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| November 2, 2012 | **Cornell University** **Ithaca, New York** | EDU | DISC | 2,000 |

Names and Social Security numbers of people associated with Cornell were publicly available for five days. The information was on a computer in Cornell's athletics department and was accidentally placed online from September 5, 2012 until September 10, 2012.

Information Source:
Media

records from this breach used in our total: 2,000

---

28 (No SSNs

| October 19, 2012 | **The College of St. Scholastica**
Duluth, Minnesota | EDU | HACK | or financial information exposed) |

Hackers were able to guess the answers to student account challenge questions. The email account passwords of at least 28 students were reset and their account information was most likely accessed. The hackers may have been based in Beijing and most likely gathered the information needed to pass the challenge questions from information on the students' Facebook pages.

Information Source: Databreaches.net

records from this breach used in our total: 0

| October 16, 2012 | **University of Georgia (UGA)**
Athens, Georgia | EDU | HACK | 8,500 |

The passwords of two University of Georgia (UGA) IT employees were reset and misused by an intruder. Names, Social Security numbers, and other sensitive data of current and former school employees may have been exposed. The breach may have begun as early as September 28, 2012.

Information Source: Media

records from this breach used in our total: 8,500

| October 15, 2012 | **District 202, Plainfield School District**
Plainfield, Illinois | EDU | HACK | 23,000 (No SSNs or financial information exposed) |

People who applied online at www.applitrack.com (http://www.applitrack.com) for a job in District 202 may have had their information accessed by a hacker. The hacker sent messages to former and current job applicants and informed them that the Plainfield School District 202 website was breached.

UPDATE (10/19/2012): A 14-year-old Joliet West High School student was removed from class and taken to a juvenile detention center for his alleged involvement in the breach.

Information Source: Databreaches.net

records from this breach used in our total: 0

| October 10, 2012 | **Northwest Florida State College**
Niceville, Florida | EDU | HACK | 279,000 (At least 200,050 SSNs exposed) |

An internal review revealed a hack of Northwest College servers. One or more hackers accessed at least one folder in the server between May 21, 2012 and September 24, 2012. Over 3,000 employees, 76,000 Northwest College student records, and 200,000 students eligible for Bright Future scholarships in 2005-06 and 2006-07 were affected. Bright Future scholarship data included names, Social Security numbers, dates of birth, ethnicity, and genders. Current and former employees that have used direct deposit anytime since 2002 may have had some information exposed. At least 50 employees had enough information in the folder to be at risk for identity theft.

Information Source: Databreaches.net

records from this breach used in our total: 200,050

| October 8, 2012 | **Ohio State University, Harvard University, Stanford University, Cornell University, Princeton University, John Hopkins University, University of Michigan, University of Wisconsin, University of Houston, New York University, University of Maryland** | EDU | HACK | Unknown |

,

There is no specific location for this breach.

The University of Texas, University of Colorado, University of Pennsylvania, Duke University, Rutgers University, University of Pittsburgh, University of Florida, Case Western Reserve University, Texas A&M University, Boston University, Purdue University, University of Arizona, Arizona State University, University of Utah, Ohio State College of Dentistry, and additional universities were affected. Universities outside of the United States were also affected.

Each affected university is listed here (http://pastebin.com/AQWhu8Ek) : http://pastebin.com/AQWhu8Ek

A hacking group called Team GhostShell targeted universities around the world. A total of 53 universities were affected. Most of the data exposed was publicly available, but student, staff, and faculty usernames and passwords were also exposed. It is unclear if any financial information or Social Security numbers were taken from universities.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| October 4, 2012 | **Monterey Institute of International Studies, Middlebury College**
Monterey, California | EDU | PORT | Unknown |

A September 14, 2012 home burglary resulted in the theft of a laptop. The laptop was password-protected and was stolen along with other items. Student names and Social Security numbers were on the laptop.

Information Source:
California
Attorney General

records from this breach used in our total: 0

| October 1, 2012 | **San Mateo Union High School District**
San Mateo, California | EDU | HACK | Unknown |

Hackers accessed San Mateo Union High School District's computer system and attempted to use it to infiltrate FBI and CIA electronic systems. The District became aware of the problem when United States Naval Intelligence informed them that the District's servers had been compromised. The hackers appear to have used additional organizations in their scheme.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| September 28, 2012 | **University of Chicago**
Chicago, Illinois | EDU | DISC | 9,100 |

A postcard mailed to University of Chicago employees contained their Social Security numbers. The cards were mailed on September 24 to remind employees about open enrollment, but also had Social Security numbers printed on the outside.

Information Source:
Databreaches.net

records from this breach used in our total: 9,100

| September 14, 2012 | **Lucille Hendricks Elementary School**
McAllen, Texas | EDU | PHYS | 20 |

A local news team was contacted when a concerned citizen noticed folders with student information in a dumpster. Former student names, Social Security numbers, dates of birth, addresses, and phone numbers were exposed. McAllen School District launched an investigation. The news team held the folders and decided to forward them to the Texas Attorney General's office.

Information Source:
Databreaches.net

records from this breach used in our total: 20

| August 28, 2012 | **Wilkinson County Schools** **Irwinton, Georgia** | EDU | HACK | Unknown |

A student was able to access and distribute information from a classroom management system called PowerTeacher. The student used user names and passwords to access grades, demographics, Social Security numbers, and other personal information. Some parents reported receiving strange calls that disclosed personal information.

Information Source: Databreaches.net

records from this breach used in our total: 0

| August 28, 2012 | **Del Mar College (East Campus)** **Corpus Christi, Texas** | EDU | PHYS | 400 |

Documents dating from 1996 to 2007 were found in a recycling bin by a student. Del Mar employee and student names, Social Security numbers, and mailing addresses were exposed. The student reported the discovery immediately and campus officials began an investigation.

Information Source: Databreaches.net

records from this breach used in our total: 400

| August 27, 2012 | **University of Rhode Island** **Kingston, Rhode Island** | EDU | DISC | 1,000 |

The University of Rhode Island released a notice on their website here (http://www.uri.edu/datanotice/) : http://www.uri.edu/datanotice/

Students and faculty who were associated with the University of Rhode island after April of 2007 may have had their personal information exposed. The information was placed on a server that was not set-up or intended to be used for storing sensitive information. The information was on the College of Business Administration's computer server and included names, Social Security numbers, dates of birth, hire year, rank, and limited compensation information. The information was discovered to be publicly accessible on July 31. It is unclear how long the information was available, but unauthorized access had occurred sometime while the information was exposed.

Information Source: Databreaches.net

records from this breach used in our total: 1,000

| August 22, 2012 | **South Bend Community School Corporation** **South Bend, Indiana** | EDU | DISC | Unknown |

A computer glitch that occurred when the district changed its student management systems caused some employee Social Security numbers to be exposed. The numbers could only be seen by other employees who were being trained on the new computer program. Employees were notified of the breach.

Information Source: Databreaches.net

records from this breach used in our total: 0

| August 21, 2012 | **Colorado State University - Pueblo** **Pueblo, Colorado** | EDU | DISC | 19,000 (No SSNs or financial information reported) |

A few students accidentally gained access to sensitive student files. It is not clear if the files were physical or electronic. The students notified school authorities immediately and the problem was fixed. It is not clear what types of student information were exposed.

Information Source:

records from this breach used in our total: 0

Databreaches.net

| August 8, 2012 | **University of Arizona (UA)**
Tucson, Arizona | EDU | DISC | 7,700 |

Those with questions may call UA's incident contact line at 520-621-4746

A UA student ran a Google search and found her private information posted publicly. The data belonged to several thousand people who had submitted their names and tax ID numbers to UA in order to receive payments or reimbursements. Vendors, consultants, guest speakers, and UA students had their names and tax ID numbers exposed in February and early March. Some people had their Social Security numbers exposed in lieu of tax ID numbers. The sensitive data was embedded within a larger set of files being transferred to the UA new financial system. The files were thought to only contain public information.

Information
Source:
Databreaches.net

records from this breach used in our total: 7,700

| August 1, 2012 | **Tarleton State University**
Stephenville, Texas | EDU | PHYS | Unknown |

Financial aid documents with student information were found scattered in the street. It is unclear how the documents got there. Hundreds of current and former students who applied for or received financial aid during 1997 and 1998 may have had their Social Security numbers, dates of birth, federal Pell grant disbursements, and other personal information exposed.

Information
Source:
Databreaches.net

records from this breach used in our total: 0

| August 1, 2012 | **Queens College**
New York, New York | EDU | HACK | 15 (No SSNs or financial information reported) |

A hacker or hackers accessed and posted sensitive information online. A total of 15 administrator user names and encrypted passwords were exposed. Three email addresses were also posted.

Information
Source:
Dataloss DB

records from this breach used in our total: 0

| August 1, 2012 | **Marquette University**
Milwaukee, Wisconsin | EDU | HACK | 15 (No SSNs or financial information reported) |

A hacker or hackers accessed and posted sensitive Marquette University information online. Fifteen names, addresses, email addresses, and passwords were exposed.

Information
Source:
Dataloss DB

records from this breach used in our total: 0

| July 25, 2012 | **Oregon State University**
Corvallis, Oregon | EDU | INSD | 21,000 |

An unnamed check printing vendor for the University copied data from the University's cashier's office during software upgrades. The information included 30,000 to 40,000 checks that contained student and employee names, University IDs, check numbers, and check amounts. Current and former student, faculty, and staff records older than 2004 may have included Social Security numbers. it does not

appear that the vendor acted with malicious intent.

*Information
Source*:
Media

records from this breach used in our total: 21,000

| July 19, 2012 | **Yale University**
New Haven, Connecticut | EDU | HACK | 1,200
(Unknown
number of
SSNs) |

Hackers accessed at least one Yale database and obtained the details of 1,200 students and staff. Hackers may have obtained names, Social Security numbers, addresses, and phone numbers. Additionally, usernames, passwords, and email addresses were published as proof of the hack.

*Information
Source*:
Databreaches.net

records from this breach used in our total: 0

| July 12, 2012 | **Scripps College Financial Aid Office**
Claremont, California | EDU | INSD | Unknown |

A former employee of Scripps College allowed a personal contact outside of the College to access financial aid application information. The issue was discovered during a review of Scripps College Financial Aid Office processes. It appears that the former employee shared the information to obtain assistance in evaluating applications and preparing potential aid packages. Names, Social Security numbers, dates of birth, and other financial information may have been exposed at various times between 2008 and 2012.

*Information
Source*:
California
Attorney General

records from this breach used in our total: 0

| July 3, 2012 | **Miami Northwestern Senior High School**
Miami, Florida | EDU | PHYS | Unknown |

A group of volunteers discovered school materials inside of a public dumpster. There were folders containing sensitive student records among textbooks, novels, and workbooks. The folders contained student Social Security numbers, health records, grade reports, and student education forms. An administrative error meant that custodians discarded obsolete materials that had been stored. The items should have been delivered to the district's central warehouse or sold to used-book dealers. The items were recovered and transmitted to the correct locations.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 0

| July 3, 2012 | **Olympic College**
Bremerton, Washington | EDU | CARD | 16 |

Those who experience an incident are encouraged to contact the college's campus security office at 360-475-7800.

Close to 20 Olympic College students and employees notified college personnel that their credit or debit card numbers were used fraudulently. The payment cards had all been used at Olympic College. The reports began in late June and the exact cause of the breach was not identified. Credit card transaction systems were removed from the main merchant network as a precaution.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 16

| July 2, 2012 | **San Jose State University (SJSU) Associated Students**
San Jose, California | EDU | HACK | Unknown |

A hacker was able to access SJSU's Associated Students information. Associated Students is a student-run non-profit that manages and hosts many SJSU campus services, but it's IT infrastructure is separate from SJSU's. The hacker claimed to have 10,000 student Social Security numbers and driver's license numbers, but it is unclear if this information was actually exposed. The hacker claimed to use an SQL injection to access the information. In addition to Social Security numbers and driver's license numbers, information such as administrative materials, job applications, work schedules, email addresses and passwords from the past 10 years may have been accessed. SJSU denies that information this sensitive was accessed.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| July 2, 2012 | **University of Florida**
Gainesville, Florida | EDU | DISC | 220 |

The University of Florida maintains a page with their privacy breach incidents here (http://privacy.ufl.edu/) : http://privacy.ufl.edu/

The information of former students and applicants was available online. Former students and applicants who signed up for a roommate service online through Levin College of Law in the early 2000s had their Social Security numbers exposed. The breach was discovered in May of 2012; the College of Law stopped using the software for the roommate service in the mid-2000s. Former students and applicants were mailed notifications on June 25.

Information Source:
Databreaches.net

records from this breach used in our total: 220

| June 29, 2012 | **University of Southern California (USC)**
Los Angeles, California | EDU | HACK | Unknown |

A breach in a third-party software system used to process credit card transactions in some USC dining halls, including Ronald Tutor Campus Center, Seeds, the Lab on Figueroa St., and Starbucks on the Health Sciences Campus resulted in the exposure of credit card numbers. The breach of USC Hospitality most likely occurred from May 21 to June 21, but may have occurred earlier. Names and contact information were not associated with the credit card numbers.

Information Source:
California Attorney General

records from this breach used in our total: 0

| June 11, 2012 | **University of North Florida (UNF)**
Jacksonville, Florida | EDU | HACK | 23,246 |

UNF Housing has set up a webpage to distribute information about the breach. It can be found here (http://www.unf.edu/housing/) .

UNF became aware of a server breach that exposed Social Security numbers and other sensitive information. Students who submitted housing contracts between 1997 and spring 2011 may have had their information exposed. Multiple servers were affected and secured upon discovery. The information may have been accessed as early as spring of 2011.

Information Source:
Databreaches.net

records from this breach used in our total: 23,246

| June 11, 2012 | **Eugene School District 4J**
Eugene, Oregon | EDU | HACK | 16,000 |

An unauthorized person accessed confidential files that contained current and former students' personal information. Names, Social Security numbers, Dates of birth, student ID numbers, phone numbers, students' free or reduced-price school lunch status, and addresses may have been exposed. Eugene School District 4J's notification can be read here (http://www.4j.lane.edu/communications/story/2012/06/11/securitybreachinformation) : http://www.4j.lane.edu/communications/story/2012/06/11/securitybreachinformation

UPDATE (07/12/2012): A minor was arrested for possible involvement in the breach. It appears that the teenager may have obtained the login credentials of an employee and used them to access the computer system. Records for approximately 16,000 current students, as well as free and reduced-price lunch records from 2007 were exposed.

UPDATE (08/25/2012): The student was released from custody and expelled by North Eugene High School. He also posted hundreds of students' confidential information on a computer account to taunt district officials. He is on house arrest and his attorney entered not guilty pleas.

Information Source:
Databreaches.net

records from this breach used in our total: 16,000

June 6, 2012	**University of Virginia** **Charlottesville, Virginia**	EDU	DISC	300 (Unknown number of SSNs)

Between 300 and 350 transcripts from Summer Language Institute applicants were accessible through the University of Virginia website. The human error was discovered when a student searched Google for an image of himself. Students who applied to the University's program within the last two years may have had their names, transcript information, and Social Security numbers exposed. Technology experts at the University blocked public access to the information and asked Google to remove its cache of the sensitive pages on June 5, 2012. It is unclear how long the information was available.

Information Source:
Databreaches.net

records from this breach used in our total: 0

June 3, 2012	**Holy Family University** **, Pennsylvania**	EDU	HACK	12 (No SSNs or financial information reported)

Holy Family University operates in the Pennsylvania cities of Philadelphia, Newtown, and Woodhaven.

A hacker or hackers accessed the database information of Holy Family University and posted the information online. The leaked data included a table with 12 usernames and encrypted passwords.

Information Source:
Dataloss DB

records from this breach used in our total: 0

May 25, 2012	**University of Nebraska, Nebraska Student Information System, Nebraska College System** **Lincoln, Nebraska**	EDU	HACK	654,000

The University of Nebraska set up a webpage for more information on the breach: http://nebraska.edu/security

A University technical staff member discovered a breach on May 23. Staff took steps to limit the breach and there was no clear evidence that any information was downloaded. The Social Security numbers, addresses, grades, transcripts, housing and financial aid information for current and former University of Nebraska students may have been accessed. The database also included the information of people who applied to the University of Nebraska, but may have not been admitted, and alumni information as far back as Spring of 1985. The University of Nebraska was still investigating the extent of the breach as of May 25, 2012.

UPDATE (05/29/2012): The University of Nebraska created a webpage (http://nebraska.edu/security) for information about the breach. Close to 21,000 people had bank account information that was linked to the student information system and exposed. The University of Nebraska's computer database also held 654,000 Social Security numbers, though it is unclear if that number completely overlaps the number of individuals who had their bank account information exposed. Current and former students of the University of Nebraska campuses in Lincoln, Omaha, and Kearney were affected; as well as anyone who applied to the University since 1985.

UPDATE (06/01/2012): The Nebraska College System began using a shared student information system called NeSIS in 2009. This resulted in data from Chadron State, Peru State, and Wayne State colleges being exposed.

UPDATE (09/10/2012): Police seized computers and related equipment belonging to a University of Nebraska-Lincoln (UNL) undergraduate student who is believed to be involved in the incident.

UPDATE (12/11/2012): The former UNL student has been charged with intentionally accessing a protected computer system and causing damage of at least $5,000.

Information Source:
Dataloss DB

records from this breach used in our total: 654,000

| May 24, 2012 | **Stanford University**
Stanford, California | EDU | HACK | 1,593 (No SSNs or financial information reported) |

A hacker or hackers accessed the database information of Stanford University and posted the information online. The leaked data included a list of contact information for donors. Names, company association, contact details, and notes about the donors were exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 18, 2012 | **University of Louisiana Monroe (ULM)**
Monroe, Louisiana | EDU | HACK | 121 (No SSNs or financial information reported) |

Anyone who participated in ULM's Upward Bound program between 2009 and 2012 should check a special ULM website for information on the breach: www.ulm.edu/breach (http://www.ulm.edu/trio/breach/) .

A University of Louisiana Monroe employee's email account was hacked. The hacker or hackers could have accessed the sensitive information of people enrolled in the Upward Bound program. A file in the employee's email included the names, addresses, telephone numbers, and other personal information of 83 high school prospects for the Upward Bound program, two former ULM employees who worked within a related program, a current ULM employee working in a related program, and 35 post-secondary ULM students.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 13, 2012 | **University of New Mexico**
Albuquerque, New Mexico | EDU | HACK | 81 (No SSNs or financial information reported) |

A hacker or hackers accessed and posted sensitive information from the University of New Mexico's electrical and computer engineering department. Usernames, emails, and encrypted passwords were exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 9, 2012 | **Tarpon Springs High School**
Tarpon Springs, Florida | EDU | DISC | 400 |

A guidance counselor accidentally sent an attachment with sensitive information to students via email. The email was sent to members of the senior class and the attachment contained the names and student ID numbers of seniors. Student Social Security numbers were used

as student ID numbers in most cases.

Information Source:
Dataloss DB

records from this breach used in our total: 400

| May 4, 2012 | **Booker T. Washington High School** **Atlanta, Georgia** | EDU | HACK | Unknown (18 students requested that their grade be altered) |

A high school student used the login credentials of his father to change student records. The student's father worked at the school as a counselor. At least 18 students paid for their attendance and course assignment records to be altered. The students who paid for the alterations were suspended. It is unclear if other students had their information accessed or altered.

Information Source:
Databreaches.net

records from this breach used in our total: 18

| May 3, 2012 | **University of Pittsburgh** **Pittsburgh, Pennsylvania** | EDU | HACK | Unknown |

Hackers associating themselves with Anonymous claimed to have obtained the private information of University of Pittsburgh students and alumni. The hackers threatened to release the information publicly unless the University apologized to students, law enforcement, and professors. The University was involved in the arrest of several supporters of Anonymous. Student passwords, dorm information, payment and credit information, parent information, coursework and grades, as well as alumni information may be exposed.

UPDATE (08/28/2012): Two men were arrested for allegedly participating in a hack of University of Pittsburgh. One entered a plea of not guilty.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| April 30, 2012 | **Volunteer State Community College** **Gallatin, Tennessee** | EDU | DISC | 14,000 |

Those with questions may call (615) 230-3390.

The University became aware of an unintended disclosure. Files with the information of current and former faculty and former students were placed on a web server that was not secure. The information could have been accessed anytime between 2008 and the discovery of the error. Names and Social Security numbers were exposed.

Information Source:
Databreaches.net

records from this breach used in our total: 14,000

| April 30, 2012 | **Columbia University** **New York, New York** | EDU | DISC | 3,500 |

A programmer erroneously saved an internal test file onto a public server in January 2010. Current and former employees had their names, Social Security numbers, addresses, and bank account numbers available on the internet from January 2010 until April of 2012. A total of 3,000 current and former employees were affected, but an additional 500 sole proprietors were also affected. It appears that the file was not accessed at anytime between January 2010 and March 10, 2012.

Information Source:

records from this breach used in our total: 3,500

Dataloss DB

| April 26, 2012 | **North East School of the Arts**
San Antonio, Texas | EDU | PORT | 1,253 |

An April 19 car burglary resulted in the exposure of student information. An external hard drive containing letters associated with students who applied to the North East School of the Arts was stolen from a teacher's car. The letters contained applicant names, Social Security numbers, dates of birth, home addresses, phone numbers, and previous school district information.

Information Source:
Dataloss DB

records from this breach used in our total: 1,253

| April 25, 2012 | **University of Alabama - Birmingham (UAB)**
Birmingham, Alabama | EDU | DISC | 8,000 |

Former students with questions may call 1-855-822-8510 or email info-help@uab.edu (mailto:info-help@uab.edu) .

People who were undergraduate students at UAB between 1995 and 2006 may have had their information accessed online. The information included Social Security numbers and academic records. It was accidentally made available on a publicly accessible server for an unspecified amount of time. The breach was discovered on March 27.

Information Source:
Dataloss DB

records from this breach used in our total: 8,000

| April 18, 2012 | **California State University San Marcos**
San Marcos, California | EDU | HACK | 700 (No SSNs or financial information reported) |

A candidate for student body president was accused of tampering with University computers in order to access student ID numbers and passwords. The information could have been used to alter election results. The University isolated and monitored the compromised accounts and rescheduled the election. The student was arrested in March on suspicion of election fraud, identity theft, and unlawful access to a computer. The student was released and no chargers were filed.

UPDATE (4/20/2012): The student was first arrested after allegedly being caught with a password stealing device at a campus computer.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 17, 2012 | **Virginia Military Institute**
Lexington, Virginia | EDU | DISC | 258 (No SSNs or financial information reported) |

A Virginia Military Institute (VMI) administrator emailed a spreadsheet with the grade point average of every member of VMI's senior class to the VMI student president. The email should have only contained an attachment with the names and hometowns of potential 2012 graduates. The second attachment was not only emailed to the student president, but was then forwarded to 258 senior students before the student president and VMI administration realized the mistake.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 14, 2012 | **Texas A&M University** **College Station, Texas** | EDU | DISC | 4,000 |

Alumni who graduated before 1985 and requested copies of their transcripts may have been affected by a breach involving accidental disclosure. Certain alumni had their names, Social Security numbers, addresses, and telephone numbers in an electronic file that was emailed to an individual who would not normally have access to such information. The person who received the email notified the University.

UPDATE (5/03/2012): This breach was erroneously listed as occurring in Corpus Christi, Texas on this site. The breach affected those who were associated with Texas A&M University in College Station, Texas.

Information Source:
Dataloss DB

records from this breach used in our total: 4,000

| April 13, 2012 | **State University of New York - Brockport College** **Brockport, New York** | EDU | HACK | 200 |

Hackers accessed Brockport College's payment system by inserting malware into Brockport College's computer system. Anyone who made a purchase on the campus may have had their credit or debit account information exposed. Brockport College responded by switching to cash payment for all purchases for the rest of the school term.

Information Source:
Dataloss DB

records from this breach used in our total: 200

| April 12, 2012 | **Housatonic Community College** **Bridgeport, Connecticut** | EDU | HACK | 87,667 |

Two campus computers were determined to have been infected by malware. The breach occurred when a faculty or staff member opened an email that contained a virus. The virus was immediately detected. Faculty, staff, and students affiliated with the school between the early 1990's and the day of the breach may have had their names, Social Security numbers, dates of birth, and addresses exposed. Housatonic's president acknowledged that the cost of handling the breach could be as much as $500,000.

Information Source:
Dataloss DB

records from this breach used in our total: 87,667

| April 11, 2012 | **ACEware Systems Inc., Lewis-Clark State College,** **Lewiston, Idaho** | EDU | HACK | Unknown |

An unauthorized party was able to access student records from ACEware Systems' server. It contained student registration records from the Lewis-Clark workforce training center.   The records included the last four digits of students' Social Security numbers and partial credit card numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 10, 2012 | **Case Western Reserve University** **Cleveland, Ohio** | EDU | PORT | 600 |

The campus theft of two university-issued laptops resulted in the exposure of alumni information. Though University policy required data security measures, the laptops were not encrypted and did not have a program installed that would allow sensitive information to be deleted remotely. Master's of arts and bachelor's of arts alumni from 1987 through the date of the theft were affected.

Information Source:
Databreaches.net

records from this breach used in our total: 600

| April 8, 2012 | **Wilson County School District**
Wilson, Tennessee | EDU | DISC | Unknown |

The names and schools of students who met with graduation coaches, as well as their reasons for meeting were not completely removed from distributed meeting materials.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 6, 2012 | **University of California Riverside**
Riverside, California | EDU | HACK | 40 (No SSNs or financial information reported) |

A hacker or hackers accessed information from the University of California Riverside. A total of 40 email addresses and corresponding passwords were posted online.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 4, 2012 | **Baylor Law School**
Waco, Texas | EDU | DISC | 442 (No SSNs or financial information reported) |

An administrative error resulted in recently admitted students receiving an email with the information of all recently admitted students. Student names, addresses, grades, LSAT scores, race, scholarship amount, and other types of personal information were available in the email attachment. No Social Security numbers or dates of birth were in the emailed spreadsheet. Students were encouraged to treat the data with the confidentiality of a lawyer and immediately delete the email.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| March 23, 2012 | **Lake Worth Independent School District**
Lake Worth, Texas | EDU | INSD | Unknown |

Employees of Lake Worth School District received email notification of a possible computer security breach. It appears that a former employee may have accessed the personal information of employees and could have misused it. It is unclear if a breach actually occurred. It is also unclear how the former employee may have compromised the district's computer system.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| March 16, 2012 | **University of Tampa**
Tampa, Florida | EDU | DISC | 30,000 |

A server management error caused files containing sensitive information to be made publicly accessible between July of 2011 and the breach's discovery on March 13, 2012. A classroom exercise revealed that the information was compromised and the University of Tampa's IT office was immediately informed of the discovery. The University of Tampa then notified Google and asked that the cached file be removed from the search engine.

One file included 6,818 records of students who attended in Fall of 2011. Two other files contained the information of an additional 29,540 people and included University ID numbers, names, Social Security numbers, and photos. Some people also had their dates of birth

exposed.The IT office at the University of Tampa concluded that the files had only been accessed by the people who reported the breach.

UPDATE (3/22/2012): Additionally, 22,722 current and former faculty, staff, and students who were associated with the University between January 29, 2000 and July 11, 2011 may have had their information exposed. The IT office confirmed that these files had only been accessed by University insiders as well. The University will not cover the cost of credit monitoring services for those who were affected.

Information Source:
Databreaches.net

records from this breach used in our total: 30,000

| March 15, 2012 | **Washington University**
St. Louis, Missouri | EDU | INSD | 4,100 |

A University employee was discovered copying electronic files onto an external hard drive on February 17, 2012. The hard drive was recovered and the employee was fired. The hard drive contained the names, Social Security numbers, addresses, and dates of birth of University employees and job applicants. It is unclear if the hard drive information was used for fraudulent purposes.

Information Source:
Dataloss DB

records from this breach used in our total: 4,100

| March 14, 2012 | **Humboldt State University**
Arcata, California | EDU | DISC | 5,700 |

The personal information of students was accidentally sent in an email attachment as a response to a request for data. The mistake was noticed immediately and all copies of the file were removed from the system of the party requesting data. Student names, addresses, and Social Security numbers were exposed. Humboldt State University warned students to be vigilant about phishing, but stated that it is unlikely the data was misused.

Information Source:
Databreaches.net

records from this breach used in our total: 5,700

| March 13, 2012 | **Brigham Young University (BYU)**
Provo, Utah | EDU | DISC | 1,300 (No SSNs or financial information reported) |

A staff member of the University Advisement Center at BYU accidentally included a complete list of international student names, email addresses, phone numbers, and student ID numbers in an email notification about a career workshop. BYU immediately apologized for the error and noted that all of the student information except for student ID numbers could easily be found in the BYU directory.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| March 7, 2012 | **Lindenwood University**
Belleville, Illinois | EDU | HACK | 184 (No SSNs or financial information reported) |

Someone accessed student information and posted it on Twitter @LindenLeaks. The information was from the Fall 2011 semester and included grades, majors, phone numbers, and email addresses. The account was eventually deleted from Twitter. The person who originally posted the information online commented that the document had been downloaded nearly 140 times since being posted.

Information Source:

records from this breach used in our total: 0

Databreaches.net

March 7, 2012	**University of California Los Angeles (UCLA)** **Los Angeles, California**	EDU	HACK	168 (No SSNs or financial information reported)

Hackers accessed and posted the usernames and passwords of individuals who had access to the UCLA.edu MySQL database. A total of 128 regular users had their names, titles, email addresses, logins, and password hashes posted online. Additionally, the IDs, usernames, salts, and password hashes from 37 staffers were posted online. Three database users also had their usernames and password hashes posted online.

Information Source:
Dataloss DB

records from this breach used in our total: 0

March 4, 2012	**Cambridge Eastern Education and Development Society (CEEDS)** **Seattle, Washington**	EDU	HACK	13 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of Cambridge Eastern Education and Development Society (CEEDS) online. The leaked data included 12 email addresses and one administrator login and (salted) password combination.

Information Source:
Dataloss DB

records from this breach used in our total: 0

March 3, 2012	**University of Washington** **Seattle, Washington**	EDU	HACK	56 (No SSNs or financial aid reported)

A team of hackers revealed that they had attacked the University of Washington's system with multiple SQL injections. The first one was detected and fixed by the University of Washington, but a second one went unnoticed. The team of hackers released 31 login and password combinations from a user database and 25 WordPress user login, password, and email address combinations. The attack comes a few weeks after a hacker identified nearly 20 university systems that were vulnerable to SQLi attacks.

Information Source:
Databreaches.net

records from this breach used in our total: 0

March 3, 2012	**Miami-Dade County Public Schools** **Miami, Florida**	EDU	INSD	Unknown

This breach was covered by the media and notifications of this breach were sent in 2009.

A former worker for the Miami-Dade school board misused student information. The dishonest employee worked as a clerk and accessed the student information for the purpose of obtaining fraudulent credit cards with her boyfriend. An unknown number of student Social Security numbers were accessed and used. She was caught in the act of stealing the Social Security numbers in 2009.

Information Source:
Media

records from this breach used in our total: 0

March 3, 2012	**Miami Central High School, Miami Northwestern High School, Golden Glades Elementary, Divine Sports Inc.**	EDU	INSD	Unknown

Miami, Florida

The media covered this breach sometime in 2011.

Divine Sports marketed itself as a non-profit that tutored at-risk youth. It appears that the owner of the company billed the Miami-Dade School District for hours of tutoring that never occurred. The company even created reports for students that did not exist by using the information of real students. Hundreds of thousands of dollars may have been fraudulently obtained over multiple years. The fraud was discovered in 2010. Divine is located in multiple states and the corporate office denied any control over the day-to-day operations of Divine Sports in Miami.

Information Source:
Media

records from this breach used in our total: 0

February 25, 2012	**Wallace Community College** **Dothan, Alabama**	EDU	HACK	284 (No SSNs or financial information reported)

Information from Wallace Community College was posted online by a hacker. The College became aware of the breach after being notified by Databreaches.net (http://www.databreaches.net/?p=23351) . Eight username, email address, and password combinations were posted in addition to 276 username, password, and full name combinations. People who used their same email and password combination for Wallace Community and other sites are encouraged to change their passwords.

Information Source:
Databreaches.net

records from this breach used in our total: 0

February 24, 2012	**Grimmer Middle School** **Schererville, Indiana**	EDU	HACK	54 (No SSNs or financial information reported)

A hacker or hackers accessed faculty and staff usernames, email addresses, and passwords. The information was then posted online.

Information Source:
Dataloss DB

records from this breach used in our total: 0

February 24, 2012	**Lake Central Clark Middle School** **Saint John, Indiana**	EDU	HACK	31 (No SSNs or financial information exposed)

A hacker or hackers accessed faculty and staff usernames, email addresses, and passwords. The information was posted online.

Information Source:
Dataloss DB

records from this breach used in our total: 0

February 22, 2012	**University of Florida** **Gainesville, Florida**	EDU	DISC	719

People who had an unclaimed check or refund from the University of Florida had their Social Security numbers posted on Florida's Unclaimed Property website. The information had been posted in July of 2005 and is from debts prior to that time, but had been posted through January 12, 2012. The University submitted its Annual Unclaimed Property Report to the Florida State Department of Financial Services. The state accidentally posted the Social Security numbers in addition to the usual information. The University of Florida was the

only entity affected by the mistake. Students, employees, and vendors may have been affected.

Information Source:
Databreaches.net

records from this breach used in our total: 719

| February 21, 2012 | **Trident University International**
Cypress, California | EDU | HACK | 81,000 (No SSNs or financial information reported) |

An unsuccessful attempt to access a database was detected by Trident University on November 29, 2011. It contained usernames and passwords of current and former students. The attempt appeared to be unsuccessful and no other information was contained in the database. Trident University offered credit monitoring services despite the belief that the attempt to access non-financial information had been unsuccessful.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| February 16, 2012 | **Central Connecticut State University (CCSU)**
New Britain, Connecticut | EDU | HACK | 18,763 |

A computer breach in a CCSU Business Office exposed the information of current and former faculty, staff, and student workers. A Z-Bot virus designed to relay information was discovered on the computer on December 6, 2011. The computer had been exposed for eight days and only exposed the Social Security numbers of those who were affected. People associated with CCSU as far back as 1998 were affected.

Information Source:
Databreaches.net

records from this breach used in our total: 18,763

| February 15, 2012 | **University of North Carolina at Charlotte**
Charlotte, North Carolina | EDU | DISC | 350,000 |

UNC-Charlotte will post information about the breach here (http://itservices.uncc.edu/home/securityincident) . Those with questions may also call (855) 205-6937.

An online security breach occurred at the UNC-Charlotte campus and was discovered on January 31. It is unclear how much information could have been accessed. The number of people affected was not revealed. An email alert was sent to students and staff on February 15 in order to inform them that a "potentially significant data exposure of its Information Systems" had occurred. The University also stated that it had corrected the known issues related to the breach.

UPDATE (5/09/2012): Around 350,000 people had their Social Security numbers exposed. Financial information was also exposed. A system misconfiguration and incorrect access settings caused a large amount of electronic data hosted by the University to be accessible from the Internet. One exposure issue affected general University systems over a period of about three months. A second exposure issue affected the college of engineering systems for over a decade.

Information Source:
Databreaches.net

records from this breach used in our total: 350,000

| February 7, 2012 | **Valencia College**
Orlando, Florida | EDU | DISC | 9,000 (No SSNs or financial information reported) |

An Excel spreadsheet with student names, addresses, dates of birth, and college ID's was listed online on a password-protected website. The password protection eventually expired and anyone could access the information online. Valencia College hired an unnamed contractor to create a custom page for prospective students to communicate with the college. The contractor then hired an unnamed sub-contractor to work on some of the website.The breach can be linked to that unnamed sub-contractor.

Information Source:
Databreaches.net

records from this breach used in our total: 0

January 31, 2012	**East Baton Rouge Acceleration Academy** **Baton Rouge, Louisiana**	EDU	UNKN	159

Police stopped a high school student and discovered several sheets of papers with student names, dates of birth, and Social Security numbers in a vehicle. It is unclear how the student obtained the printout and she is accused of using the information to file fraudulent federal income tax returns.

Information Source:
Databreaches.net

records from this breach used in our total: 159

January 29, 2012	**Palos Verdes High School** **Palos Verdes, California**	EDU	HACK	Unknown

Three students were caught selling quiz answers to students. It was discovered that they had stolen and copied a master key from the janitor's office. They then used the copy of the master key to install keylogging hardware onto the computers of four teachers. The keylogging hardware revealed passwords, which were then used to access the central files of the school network. It is unclear what types of information the students had access to. They used their access to electronically change their grades slightly. The master key copy was also used to access 20 paper tests before they were given. A student who became aware of the black market for quiz materiala reported the students.

Information Source:
Databreaches.net

records from this breach used in our total: 0

January 28, 2012	**Naperville Unit District 203** **Naperville, Illinois**	EDU	DISC	101 (No SSNs or financial information reported)

The report cards of 101 high school students were accidentally sent to the person listed as their emergency contact. A vendor made an unauthorized change to the computer program that generates report cards. If a parent had a high school student attending the district and was listed as an emergency contact for another high school student, then they received two report cards. Parent names were listed on the report cards of each student, but parents listed as emergency contacts mistakenly received the report cards anyway. No Social Security numbers were exposed. Student ID numbers, schedules, and grades were exposed.

Information Source:
Databreaches.net

records from this breach used in our total: 0

January 20, 2012	**Arizona State University (ASU)** **Tempe, Arizona**	EDU	HACK	300,000 (No SSNs or financial information reported)

ASU online system users with questions about logging into their accounts may call (855) 278-5080.

ASU shutdown its online computer system after discovering a breach. An encrypted file containing user names and passwords was

downloaded on Wednesday, January 18 by an unauthorized party. All online services were suspended until the night of Thursday, January 19. Students and staff will be required to enter new passwords to access their accounts since there is a chance that some information could have been compromised.

Information Source:
Databreaches.net

records from this breach used in our total: 0

January 13, 2012	**City College of San Francisco** **San Francisco, California**	EDU	HACK	Unknown

The College's electronic systems have been affected by a series of dangerous viruses since 1999. The problem was noticed in 2012 when the College's data security monitoring service detected an unusual pattern of computer traffic. Further investigation revealed that servers and desktops had been infected across administrative, instructional, and wireless networks. Officials believe that it is likely that using a flash drive to transmit information between a campus computer and a personal computer resulted in exposed personal information. It appears that the viruses searched and transmitted data to sites in Russia, China, and at least eight other countries. Banking information and any other personal information that may have been accessed by visitors, students, staff, and faculty on campus computers between 1999 and January of 2012 could have been exposed.

Information Source:
Databreaches.net

records from this breach used in our total: 0

January 10, 2012	**Isaac Miller Elementary School, Santa Maria-Benita School District** **Santa Maria, California**	EDU	PHYS	Unknown

A man noticed dozens of books and documents inside a dumpster near Miller Elementary. The documents contained personal and financial information related to applications for free and recuded-price meals. The books were new and federally-funded. School officials claimed that the documents should have been shredded and recovered the documents and books. The books were donated.

Information Source:
Databreaches.net

records from this breach used in our total: 0

January 6, 2012	**Spotsylvania County** **Spotsylvania, Virginia**	EDU	DISC	4,289

An employee discovered that it was possible to access current and former employee W-2 forms online via a Google search. The W-2 form contained employee name, Social Security number, address, earnings, and taxes paid for 2009 and 2010. The discovery was made on December 23 of 2011.

Information Source:
Media

records from this breach used in our total: 4,289

December 15, 2011	**Jefferson County Public Schools** **Louisville, Kentucky**	EDU	DISC	6,500 (No SSNs or financial information exposed)

Around 6,500 ACT Explore test results for 8th graders were mailed to incorrect addresses. The breach was discovered when parents began calling the district. Parents were asked to shred the tests. The exact cause of the mailing error is unknown.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| December 2, 2011 | **University of Kansas (KU)** **Lawrence, Kansas** | EDU | PHYS | Unknown |

Documents containing the personal information of current and former student housing residents was stolen during a burglary at the Department of Student Housing office on November 30. Names, dates of birth, apartment numbers, email addresses, KU ID numbers, and other information, some of it related to student dependents, were on the documents. The number of affected students was not revealed, but those who were affected were told to be cautious of identity theft.

Information Source: Databreaches.net

records from this breach used in our total: 0

| November 30, 2011 | **The College of New Jersey** **Ewing, New Jersey** | EDU | DISC | 12,815 (No SSNs or financial information reported) |

The College's On-Campus Student Employment System had a vulnerability that allowed student applicants to see the personal information of other students. A student applicant notified the College of the problem on November 2 after seeing the information of 12 other students. The system flaw was fixed within hours, but no duration was given for the breach.

Information Source: Databreaches.net

records from this breach used in our total: 0

| November 29, 2011 | **University of California Riverside (UCR)** **Riverside, California** | EDU | HACK | 5,000 |

Those with questions may call 1-855-827-2277.

Several customers of the UCR Dining Services location reported fraudulent credit and debit card activity to UCR. On or around November 16, it became clear that registers at UCR food services locations were compromised by a cyber hacker. Anyone who used a card, including visitors, between the summer of 2011 and November 16, 2011 may have had their financial information obtained. The information includes cardholder names, numbers, expiration dates, and an encrypted version of debit PINs.

Information Source: Databreaches.net

records from this breach used in our total: 5,000

| November 23, 2011 | **MassBay Community College** **Wellesley, Massachusetts** | EDU | DISC | Unknown |

A glitch allowed nearly 400 workers from 2002 to 2011 to view the personal information of any employees in MassBay's worker database system. The information included Social security numbers, home addresses, and other personnel information.

Information Source: Databreaches.net

records from this breach used in our total: 0

| November 21, 2011 | **Blairsville High School** **Blairsville, Pennsylvania** | EDU | HACK | Unknown |

Two students managed to obtain the login credentials for Blairsville High's online security system by repeatedly guessing. Their attempts began in May and were only discovered during the fall term when one of the students revealed his teacher's Social Security number in class. Teacher addresses, Social Security numbers, and salaries were exposed.

Information Source:

records from this breach used in our total: 0

Databreaches.net

November 14, 2011	**Santa Clara University** **Santa Clara, California**	EDU	HACK	60 (No SSNs or financial information reported)

The academic records database of Santa Clara University was hacked in order to change the grades of over 60 current and former undergraduate students. The breach was discovered when a former student pointed out that her current transcript showed a grade better than the one on a transcript that had previously been printed. Tens of thousands of student records dating back more than a decade were examined. The "sophisticated" hacking incident or incidents had altered student transcripts from all three of the University's schools and changed some grades for courses taken as far back as 2006. The incident or incidents is believed to have occurred between June 2010 and July 2011. Some students received subtle upgrades and others had their grades changed from F's to A's.

Information Source: Databreaches.net

records from this breach used in our total: 0

November 13, 2011	**Brownsville Independent School District** **Brownsville, Texas**	EDU	DISC	Unknown

Affected employees may call (965) 548-8061.

Brownsville ISD discovered that a number of employees had their names, Social Security numbers, disability plan information, and salary information available on a publicly accessible website. Employees who were enrolled for disability insurance had their information posted in April 2011 on the Employee Benefits/Risk Management website.

Information Source: Databreaches.net

records from this breach used in our total: 0

November 11, 2011	**University of Texas-Pan American** **Edinburg, Texas**	EDU	DISC	19,276 (No SSNs or financial information reported)

Those with questions may email infosecurity@utpa.edu (mailto:infosecurity@utpa.edu) .

On September 1, 2011, a spreadsheet containing information on 19,276 students was accidentally made accessible from the internet due to a administrative error. The spreadsheet contained the names, addresses, phone numbers, email addresses, majors, class or classes, levels, colleges, student ID numbers, and GPAs of students enrolled as of September 1 of 2011. The problem was corrected on November 2 soon after it was discovered. The spreadsheet had been accessed 15 times by unknown parties between September 1 and November 2.

Information Source: Databreaches.net

records from this breach used in our total: 0

November 11, 2011	**Virginia Commonwealth University** **Richmond, Virginia**	EDU	HACK	176,567

Those with questions may call (855) 886-2931 or email responseteam@vcu.edu (mailto:responseteam@vcu.edu) .

Hackers were able to access a Virginia Commonwealth University (VCU) computer server. It contained files with the personal information of current and former VCU and VCU Health System faculty, staff, students and affiliates. Suspicious files were discovered on the server on October 24. It was taken offline and subsequent investigation revealed that two unauthorized accounts had been created on a second server. While the first server did not contain personal data, the second server did and had been compromised through the first server.
 Data included either a name or eID, Social Security number, and in some cases, date of birth, contact information, and various programmatic or departmental information.

Information *Source*: Databreaches.net				*records from this breach used in our total: 176,567*

November 10, 2011	**Wakulla County School Board** **Crawfordville, Florida**	EDU	DISC	2,400

The information of 2,400 students in grades four through ten was accidentally posted online. A parent discovered the breach after searching their child's name. The student's FCAT scores and Social Security number appeared on a public site. The cause of the unintended disclosure was not reported.

Information *Source*: Databreaches.net				*records from this breach used in our total: 2,400*

November 2, 2011	**University of Alabama** **Tuscaloosa, Alabama**	EDU	DISC	Unknown

On October 26, students who had at least one failing midterm grade during the Fall 2011 semester received an email from the office of the assistant dean of students. The email, which informed students of their grade, was not blind copied. Each email recipient could see the email addresses of other students who received the email. No other information was exposed.

Information *Source*: Databreaches.net				*records from this breach used in our total: 0*

October 20, 2011	**College of the Holy Cross** **Worcester, Massachusetts**	EDU	UNKN	493

Seven Holy Cross employees fell for phishing attempts. The employees had their email accounts attacked and emails containing personal information for hundreds of people were exposed. Though Holy Cross has a policy of encrypting all emails that contain personal information, these emails were not encrypted. Those who could have been affected were notified that their Social Security numbers, driver's license numbers, dates of birth, financial information and other types of information were at risk.

Information *Source*: Databreaches.net				*records from this breach used in our total: 493*

October 10, 2011	**University of Georgia (UGA)** **Athens, Georgia**	EDU	DISC	18,931

A data file that contained employment information such as names, Social Security numbers, dates of birth, dates of employment, gender, race, home phone numbers, and addresses was accidentally placed on a publicly available web server. The information was available from 2008 until 2011. Faculty and staff who worked at UGA in 2002 were affected.

Information *Source*: Media				*records from this breach used in our total: 18,931*

September 23, 2011	**University of Texas San Antonio (UTSA)** **San Antonio, Texas**	EDU	DISC	688 (No SSNs or financial information reported)

Students and prospective students who enrolled in or applied to courses in UTSA's Honors College may have had their information exposed. On August 2, a UTSA employee discovered that a system misconfiguration allowed unauthorized users to access names, dates of birth, addresses, phone numbers, email addresses, GPAs and other personal information of students and prospective students. Between

June 20 and August 2, Honors College users as well as all other UTSA employees with access to the online system could view student information.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| September 16, 2011 | **Xavier University**
Cincinnati, Ohio | EDU | PHYS | Unknown |

Sensitive student athlete medical records were misplaced by a coach who was transplanting them to an athletic event. A recently released prisoner found the documents and attempted to sell them back to the University for $20,000. The man was caught, pled guilty to extortion, and was sentenced to two years in prison.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 0

| September 9, 2011 | **Indiana University School of Medicine**
Indianapolis, Indiana | EDU | PORT | 3,192 (178 cases of Social Security numbers) |

A laptop with sensitive information was stolen from a physician's car on Tuesday, August 16 of 2011. It contained patient information such as name, age, sex, diagnosis, medical record number, and in 178 cases, Social Security numbers. Individuals were notified on September 2.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 178

| September 1, 2011 | **Birdville**
Haltom City, Texas | EDU | HACK | 14,500 |

Two students may face criminal charges for hacking into the Birdville School District's network server and accessing a file with 14,500 student names and Social Security numbers. The students are a high school junior and a senior. Students who attended during the 2008-2009 school year may have been affected.

Information Source:
Databreaches.net

records from this breach used in our total: 14,500

| September 1, 2011 | **Harvard University**
Cambridge, Massachusetts | EDU | DISC | Unknown |

Harvard's switch to Google "@college" email accounts resulted in the potential compromise of some student emails. Fewer than ten students reported that emails from other students with similar names were forwarded to them. The problem occurred because the email system did not distinguish between the older "@fas" accounts and the newer "@college" accounts. For example, the system would forward emails from ctucker@fas.harvard.edu (mailto:ctucker@fas.harvard.edu) to the new address of ctucker@college.harvard.com (mailto:ctucker@college.harvard.com) even if the "@harvard" email had been taken by a different student. Students with "@harvard" emails also had their emails forwarded to other students' accounts.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| September 1, | **El Paso Independent School DIstrict (EPISD)** | | | 72,000 (26 |

| 2011 | **El Paso, Texas** | EDU | HACK | confirmed cases) |

Hackers accessed the EPISD server and were able to collect the personal information of students, teachers and other employees. There were names, Social Security numbers, and addresses from approximately 63,000 students and 9,000 teachers on the district's internal network (myepisd.org). EPISD was not aware of the breach until a computer security company noticed hackers bragging about breaking into EPISD's system. Names, ethnicity codes, and student ID numbers for 26 students were posted by hackers named Sy5t3mF41lur3 & t3hblackhatter of H05t_Bu5t0rz.

UPDATE (09/07/2012): A hacker accused of carrying out the attack is scheduled to plead guilty to two counts of computer fraud and one count of fraud linked to identification documents.

Information Source:
Databreaches.net

records from this breach used in our total: 72,000

| August 17, 2011 | **Yale University**
New Haven, Connecticut | EDU | DISC | 43,000 |

A computer file containing the names and Social Security numbers of former faculty, staff and students was accidentally made accessible online. The file contained information from 1999 and could be located through a Google search for 10 months. A change in Google's search engine made the file accessible from September 2010 to July 1, 2011. A person who performed a Google search on his name discovered the breach on June 30.

Information Source:
Databreaches.net

records from this breach used in our total: 43,000

| August 16, 2011 | **Purdue University**
West Lafayette, Indiana | EDU | HACK | 7,093 |

An unauthorized person broke into Purdue's computer system on April 5, 2010, and tried to use the server to attack other servers. Purdue staff learned of the breach three days latter and began an assessment. The server was taken offline and staff later determined that Social Security numbers belonging to current and former students who took mathematics courses and a limited number of faculty, faculty family members and contractors were exposed. The Social Security numbers were then matched to their owners and notification was sent to the Attorney General's office in June of 2011.

Information Source:
Databreaches.net

records from this breach used in our total: 7,093

| August 15, 2011 | **North Carolina State University (NCSU), Gardners Elementary School, Wells Elementary School, Ashley Chapel Elementary School**
Raleigh, North Carolina | EDU | DISC | 1,800 |

A server that contained data from school children in Wilson and Richmond counties was mistakenly put online. The information was gathered between 2003 and 2006 as part of a research study on classroom practices. It included names, Social Security numbers and dates of birth. A concerned parent notified the state Department of Public Instruction after finding the information online. The error was fixed in July, though it is unclear how long the information was available online.

Information Source:
Databreaches.net

records from this breach used in our total: 1,800

| August 13, 2011 | **University of Hawaii - Kapi'olani Community College**
Honolulu, Hawaii | EDU | PHYS | 2,000 |

A worker noticed that boxes of sensitive financial records were out of place. Some boxes were discovered to be missing and officials began searching for them on July 1. The breach was reported to students during the first week of August. It is unclear when the boxes were taken and there was no sign of forced entry into the area where they were stored. The files contained names, addresses, Social Security

numbers and credit cards. People who made transactions with credit cards between February and November of 2010 for non-credit classes, transcript requests, or payment of non-resident fees were effected.

Information Source:
Databreaches.net

records from this breach used in our total: 2,000

| August 10, 2011 | **University of Wisconsin - Milwaukee**
Milwaukee, Wisconsin | EDU | HACK | 79,000 |

On May 25, University technology staff learned that unauthorized individuals had installed computer viruses on a University server. It housed a software system for managing confidential information. The names and Social Security numbers or people associated with the University could have been exposed. There was no evidence that unauthorized parties had attempted to download the confidential information.

Information Source:
Databreaches.net

records from this breach used in our total: 79,000

| August 10, 2011 | **Cal Poly Pomona**
Pomona, California | EDU | DISC | 38 |

On August 2, a lecturer working in a student lab discovered that two files on a server could be accessed by faculty members, staffers and students from the College of Business Administration. The files were confidential and included personal information such as names and Social Security numbers. A total of 38 current and former faculty members were affected by the breach. The University determined that the information had not been digitally copied by anyone.

Information Source:
Databreaches.net

records from this breach used in our total: 38

| August 1, 2011 | **University of North Carolina - Chapel Hill**
Chapel Hill, North Carolina | EDU | PHYS | 30 (No SSNs or financial information reported) |

Someone broke into the UNC-Chapel Hill judicial office and took the files of 30 students. The break-in was discovered at the beginning of the day on Monday. University student affairs officials contacted each of the students who had their records stolen.

UPDATE (8/9/2011): A suspect was caught. He was arrested on charges of breaking-and-entering, larceny and possession of stolen goods.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| July 31, 2011 | **Tufts University, Massachusetts General Hospital (MGH)**
Boston, Massachusetts | EDU | PORT | Unknown |

A research associate's laptop was stolen during the course of research with a Tufts professor. The research was being conducted at MGH. The laptop was mostly used for research, but a sensitive file had been uploaded in early 2010. It contained a spreadsheet with the information of applicants who applied to the Graduate School of Arts and Sciences at Tufts. Applicant Social Security numbers were included in the spreadsheet. The theft occurred in April of 2011 and was reported to MGH. Tufts learned of the breach on June 16, 2011.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| July 26, 2011 | **University of Nevada - Las Vegas (UNLV)**
Las Vegas, Nevada | EDU | HACK | 2,000 |

Current and former UNLV employees may have been affected by a breach. It is possible that an unauthorized user gained access to a former employee's computer in December of 2008. Employee information that included Social Security numbers would have been exposed. The potential breach was discovered in 2011 during maintenance on a computer in UNLV's Controller's Office.

Information Source:
Databreaches.net

records from this breach used in our total: 2,000

| July 7, 2011 | **Clark College**
Vancouver, Washington | EDU | HACK | 250 (9 SSNs exposed) |

An unauthorized access resulted in the exposure of faculty, student and staff information. Student names and identification numbers were exposed. The types of faculty and staff information that may have been exposed were not reported.

Information Source:
Databreaches.net

records from this breach used in our total: 9

| June 24, 2011 | **Harrisburg Project, West Aurora School District, Kaneland School District**
Palatine, Illinois | EDU | PORT | 10,000 |

The West Aurora school district headquarters is in Aurora, Illinois and the Kaneland school district is in Maple Park, Illinois. The theft occurred in Palatine, Illinois.

Two laptops were stolen from a car on or around June 7. The laptops were from an Illinois State Board of Education (ISBE) subcontractor called Harrisburg Project. The ISBE uses the Harrisburg Project as a subcontractor for special education reimbursement purposes. The laptops contained the personal information of over 10,000 students and staff from northern Illinois. Employees were using the laptops for training in data entry.

UPDATE (6/29/2011): It appears that both student and staff Social Security numbers were on the laptops. Additionally, student names, dates of birth, residential school district and other educational information were on the laptops. Staff names, demographics, teacher certification numbers and work assignments were on the laptops.

Information Source:
Databreaches.net

records from this breach used in our total: 10,000

| June 23, 2011 | **University of Central Missouri**
Warrensburg, Missouri | EDU | HACK | Unknown |

Two former students conspired to obtain and sell large databases of faculty and alumni information, change grades and steal funds from the accounts of other students. The two students developed malware that allowed them to capture passwords and gain unauthorized access to the University's network. The students were able to install the malware in a variety of ways. For example, the students obtained the information of other students by inserting a thumb drive into public PCs and personal laptops. Malware was installed on at least one University administrator's computer and the login credentials of a residence hall director were stolen.

One of the men pleaded guilty to charges of computer hacking conspiracy and computer intrusion. Charges are pending against the student's alleged accomplice.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| June 14, 2011 | **St. Louis University (SLU)**
St. Louis, Missouri | EDU | PHYS | Unknown |

Someone noticed a pile of discarded paperwork and informed a local news station after it had not been removed within a week. Documents with the personal information of dozens of former St. Louis University students were exposed near a dumpster in a back alley. Most appeared to date back to the mid 1990's and correspond to library fines for late or lost books. An SLU security team picked up the papers after hearing about the incident.

*Information
Source*:
Databreaches.net

records from this breach used in our total: 0

| June 11, 2011 | **Penn State Altoona**
Altoona, Pennsylvania | EDU | HACK | 12,000 |

A virus infected a Penn State Altoona computer that contained the names, addresses and Social Security numbers of alumni, faculty and staff members. The virus appeared on the computer sometime during the spring semester and was discovered on March 15. Those who were affected were not notified until June because the full list of affected people and their contact information had to be obtained by investigators. Only alumni with identical Social Security numbers and student IDs were affected.

*Information
Source*:
Databreaches.net

records from this breach used in our total: 12,000

| June 10, 2011 | **Ravenel Elementary School**
Seneca, South Carolina | EDU | PORT | 15 |

A Memorial Day weekend office burglary resulted in the theft of two laptops and a flash drive. The flash drive may have contained student information. This potential exposure includes copies of Medicaid release forms with student names, parent names and Medicaid numbers.

*Information
Source*:
Databreaches.net

records from this breach used in our total: 15

| June 8, 2011 | **University of Mary Washington (UMW)**
Fredericksburg, Virginia | EDU | DISC | 7,566 |

Students with questions may call University officials at 540-654-1265 or 540-654-2246.

A student discovered student data files on a departmental EagleNet site while searching the EagleNet portal for his own information. A total of three students accessed the sensitive files and were interviewed. Student names, Social Security numbers and dates of birth were accessible. The information was accidentally placed their by a faculty or staff member and reported on May 23.

*Information
Source*:
Databreaches.net

records from this breach used in our total: 7,566

| May 27, 2011 | **San Juan Unified School District**
Carmichael, California | EDU | DISC | 4,000 |

A human resources employee of San Juan Unified uploaded sensitive employee information onto a flash drive. Somehow the information was uploaded onto a website when the employee used the flash drive to perform volunteer work at her church. An employee who Googled their own name discovered that they could also see their Social Security number and other sensitive information. The information was available for six months.   San Juan Unified decided to ban flash drives as a result of the incident.

*Information
Source*:
Databreaches.net

records from this breach used in our total: 4,000

| May 20, 2011 | **Excel Academy**
Castroville, Texas | EDU | INSD | Unknown |

A group of employees left Excel Academy and took student information with them to a rival organization. School district superintendents were solicited by the rival academy, Eagle Wings, and shown student information that Eagle Wings should not have possessed. Student names and Social Security numbers were exposed. Excel reported the incident and police launched an investigation. Excel has student information from 33 districts.

Information Source: Databreaches.net				*records from this breach used in our total: 0*

May 9, 2011	**Eastern Illinois University** **Las Vegas, Nevada**	EDU	PHYS	Unknown

Partially-shredded personnel records were dumped alongside a roadside. Names and Social Security numbers from University employees employed during 2002 were exposed.

A student employee from the Records Management Office had taken two bags of personnel documents for use in a prank. Both bags were eventually found.

Information Source: Databreaches.net				*records from this breach used in our total: 0*

May 7, 2011	**Central Oregon Community College (COCC)** **Montpelier, Vermont**	EDU	HACK	Unknown

Those with questions may call 541-383-7599.

COCC's website experienced an unauthorized intrusion. Students who applied to the COCC nursing program for the current school year, and for a COCC Foundation scholarship for the following school year may have had their personal information exposed. The potentially exposed information does not include Social Security numbers, credit card numbers, email addresses or COCC ID numbers. It is unclear which information may have been exposed.

Information Source: Databreaches.net				*records from this breach used in our total: 0*

May 4, 2011	**Catholic Social Services** **,**	EDU	PORT	1,700 (No SSNs or financial information reported)

The February 1 theft of a contractor's laptop may have exposed client personal and health information. The laptop was stolen from the car of an out of state contractor working for the Pregnancy Support and Adoption Services program. It contained personal information that included names, addresses, phone numbers, email addresses, dates of birth, driver's license information, health information, family histories, financial statuses and recommendation for readiness to adopt. Individuals who requested a home study in order to adopt a child between 2008 and 2010 were among those affected.

Information Source: HHS via PHIPrivacy.net				*records from this breach used in our total: 0*

April 19, 2011	**Central Ohio Technical College (COTC)** **Newark, Ohio**	EDU	PHYS	617

An enclosed file cabinet with student registration cards was left unattended for a short period of time. The cabinet was moved to a temporary storage facility while the Student Records Management Office prepared to move to a new location in the same building. The cabinet should not have been left unattended; it contained Social Security numbers for students who registered for the fall quarter of 2010 at any COTC campus. The incident occurred on March 10 and notifications were sent to students on April 14.

Information Source: Databreaches.net				*records from this breach used in our total: 617*

| April 13, 2011 | **Albright College**
Reading, Pennsylvania | EDU | PORT | 10,000 |

Two laptops were stolen from the College's financial aid office in February. The first laptop was stolen between February 11 and 14. The second was stolen between February 18 and 20. College officials delayed notifying the public of the incident until a risk management firm had assessed the extent of the breach. The laptops contained names, Social Security numbers, dates of birth and addresses. The information may have belonged to faculty, staff, graduates, current and prospective students, spouses of any of these groups and parents of students. The laptop believed to have the most personal information was recovered from a man who was selling the item for drug money.

Information Source:
Databreaches.net

records from this breach used in our total: 10,000

| March 26, 2011 | **Killeen Independent School District (KISD)**
Killeen, Texas | EDU | PHYS | 58 |

A man found student documents near a freeway. A list of student names and their Social Security numbers was found; but it is unclear if teacher evaluations and grade books were also found. KISD said that there were no specific policies for shredding confidential KISD information.

UPDATE (4/13/2011): Notification letters were sent to the homes of 58 students. The Social Security numbers of those students may have been exposed.

Information Source:
Databreaches.net

records from this breach used in our total: 58

| March 22, 2011 | **Laredo Independent School District**
Laredo, Texas | EDU | PORT | 24,903 |

A disk that contained the Social Security numbers of all students in the Laredo Independent School District was lost or stolen sometime prior to February of 2011.

UPDATE (4/7/2011): Between August 2010 and January 2011, CDs that were mailed to the Texas Education Agency (TEA) were lost. The CDs were unencrypted and contained student Social Security numbers, dates of birth and ethnicity. The CDs were sent to TEA so that identifying information could be removed and the information could be passed along to the University of Texas at Dallas Education Research Center. According to a TEA spokesperson, Laredo ISD's data set is missing from a set of other district information that was sent. Though the TEA claims that only Laredo student information was exposed, the information of 164,406 students from eight Texas school districts was sent. The information on the unencrypted disks goes back 20 years. This information includes current and former students in the top 10% of their class who graduated between 1992-2010 from Crowley, Harlingen, Round Rock, Killeen, Richardson, Irving, Mansfield, and Grand Prairie school districts.

Information Source:
Databreaches.net

records from this breach used in our total: 24,903

| March 21, 2011 | **Tesoro High School**
Las Flores, California | EDU | HACK | unknown |

A 21-year old was sentenced to jail after it was discovered that he had broken into his high school's computer system in 2008. He stole tests and changed his grades. He was ordered to pay $15,000, serve 30 days in jail and serve 500 hours of community service.

UPDATE (8/26/2011): The former student successfully paid the fine in August.

Information Source:
Media

records from this breach used in our total: 0

March 16, 2011	**St. Louis University** **St. Louis, Missouri**	EDU	HACK	12,800

The University's network was hacked on December 12, 2010. The breach was discovered on December 13 and a statement was available on the University's website on January 31, 2011. Eight hundred students and 12,000 current and former employees and contractors were affected. Only people who worked for Saint Louis University at some point had their Social Security numbers exposed. Some students who received counseling through the University's Student Health Services may have had their names, dates of birth, tests, diagnosis and treatment information exposed.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 12,000

March 14, 2011	**Virginia Polytechnic Institute and State University (Virginia Tech)** **Blacksburg, Virginia**	EDU	HACK	370

A virus infected a Virginia Tech computer on February 15 and sent Social Security numbers and some financial information overseas. The virus was discovered on February 23. Certain current and former employees were affected.

Information Source:
Databreaches.net

records from this breach used in our total: 370

March 10, 2011	**University of Massachusetts Amherst, University Health Services** **Amherst, Massachusetts**	EDU	HACK	Unknown

A workstation at the campus University Health Services (UHS) was infected with malware. The work station contained patient names, health insurance company names, medical record numbers, and prescription information from January 2, 2009 to November 17, 2009. There is no evidence that the data was copied from the workstation. The malware was on the computer from June 30, 2010 to October 28, 2010. Patients were notified in March.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 0

March 9, 2011	**Chapman University** **Orange, California**	EDU	DISC	Unknown

A file that should have only been available to certain University system users was available to all users. It contained the names, Social Security numbers, student ID numbers and financial aid information of students who applied for financial aid for the 2009-2010 school year.

Information Source:
Databreaches.net

records from this breach used in our total: 0

March 9, 2011	**Eastern Michigan University** **Ypsilanti, Michigan**	EDU	INSD	45

Two former student employees may have obtained student information and provided it to outsiders. Names, Social Security numbers and dates of birth may have been exposed.

UPDATE (10/25/2011): A former student was charged with eight counts of felonies related to the breach. The charges include identity theft and using a computer to commit a crime. A warrant was issued for a second student.

Information Source:
Databreaches.net

records from this breach used in our total: 45

March 8, 2011	**Western Michigan University** **Kalamazoo, Michigan**	EDU	PORT	Unknown

A backup hard drive that contained student and faculty information was discovered missing on January 25. Hundreds of current and former students and faculty members had their names and Social Security numbers exposed by the breach. Academic records were also on the hard drive.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| March 4, 2011 | **University of South Carolina** **Sumter, South Carolina** | EDU | HACK | 31,000 |

A computer security problem may have exposed the information of faculty, staff, retirees and students on eight University system campuses. Social Security numbers and other private information could end up on the internet.

Information Source:
Databreaches.net

records from this breach used in our total: 31,000

| March 3, 2011 | **Missouri State University** **Springfield, Missouri** | EDU | DISC | 6,030 |

Nine student lists were accidentally placed on an unsecured server in October and November of 2010. The problem was noticed on February 22. The College of Education lists of students between 2005 and 2009 contained names and Social Security numbers.

Information Source:
Databreaches.net

records from this breach used in our total: 6,030

| February 23, 2011 | **Chapman University, Brandman University** **Los Angeles, California** | EDU | DISC | 13,000 |

A student discovered a document with sensitive information in an unsecured folder. It contained names, Social Security numbers, student ID numbers and financial aid information. Around 11,000 current and former Chapman students, 1,900 applicants and an unspecified number of Brandman students were affected. Only students and people affiliated with the University could have accessed the file, and it appears that the student who reported the incident was the only one who accessed the file.

Information Source:
Databreaches.net

records from this breach used in our total: 13,000

| February 3, 2011 | **University of Washington Hospital** **Seattle, Washington** | EDU | PHYS | 17 (No SSNs or financial information reported) |

A customer purchased a piece of furniture from the University's Surplus Store that had the medical records of patients. The information in the records was mostly x-ray and MRI images of spines.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 0

| January 26, 2011 | **Warner Pacific College** **Portland, Oregon** | EDU | PORT | 1,536 |

A laptop was stolen from an employee's home on January 3. It contained the names, Social Security numbers, dates of birth, telephone numbers and addresses of students.

Information

Source: Databreaches.net			*records from this breach used in our total: 1,536*

January 26, 2011	**Universal Technical Institute** **Phoenix, Arizona**	EDU	PORT	98

The names and Social Security numbers of recent applicants were on a stolen laptop. The laptop was stolen from UTI's Phoenix office on November 18. Some applicants may have had their dates of birth and contact information exposed as well.

Information Source: Databreaches.net			*records from this breach used in our total: 98*

January 25, 2011	**Plainfield Board of Education** **Plainfield, New Jersey**	EDU	UNKN	Unknown

Someone posted administrative login information and a link to the login page of the Plainfield District's Genesis Student Information System on a popular online message board. Plainfield did not disclose how the admin user name and password were discovered. An unknown number of people would have had access to student records and maybe even student and parent contact information. The breach was discovered and addressed within 24 hours.

Information Source: Databreaches.net			*records from this breach used in our total: 0*

January 24, 2011	**Wentworth Institute of Technology** **Boston, Massachusetts**	EDU	DISC	1,300

On December 22 of 2010, Wentworth became aware of a breach that left sensitive student information online. A file was accidentally placed on Wentworth's website at some point. Current and former students may have had their names, Social Security numbers, dates of birth and medical information exposed.

Information Source: PHIPrivacy.net			*records from this breach used in our total: 1,300*

January 24, 2011	**University of Missouri, Coventry Health Care** **Columbia, Missouri**	EDU	DISC	750 (No SSNs or financial information reported)

A Coventry Health Care computer malfunction caused the names of University of Missouri health insurance program participants to be aligned with incorrect mailing addresses. Names, member numbers and birth dates were on mailed documents like benefits statements, health services letters and new ID cards. The erroneous mail was sent out to employees between January 6 and 10. An employee notified the University on or around January 14.

Information Source: PHIPrivacy.net			*records from this breach used in our total: 0*

January 18, 2011	**Tulane University** **New Orleans, Louisiana**	EDU	PORT	10,000

A University issued laptop was stolen from an employee's car on December 29. The laptop was used to process 2010 tax records for employees, students and others who will receive a 2010 W-2. The information included names, Social Security numbers, salary information and addresses.

Information Source: Databreaches.net	*records from this breach used in our total: 10,000*

January 15, 2011	**Omaha School Employees Retirement System** **Omaha, Nebraska**	EDU	HACK	4,300

A breach of Omaha School Employees Retirement System's website was discovered on December 21. The incident occurred because of an attempt to access administrator log-in information. The hacker or hackers may have obtained a database with names, Social Security numbers, dates of birth, years of service and beneficiary information of current and former Omaha Public Schools employees. The website was shut down within two hours of the discovery.

Information Source: Databreaches.net	*records from this breach used in our total: 4,300*

January 11, 2011	**University of Connecticut, HuskyDirect.com** **Storrs, Connecticut**	EDU	HACK	18,059

Customers who used their credit cards on UConn's Huskydirect.com sports gear website may have had their personal information exposed in a data security breach. A hacker was able to access the Huskydirect.com customer database and may have viewed billing information with names, addresses, telephone numbers, credit card numbers, expiration dates, security codes and email addresses. The Huskydirect.com database is run by an outside vendor. People who made purchases offline are not at risk.

UPDATE (1/31/2011): Some people who were affected by the breach have recently reported fraudulent charges.

UPDATE (2/19/2011): Additional details reveal the exact number of names that were on the customer database, the fact that the perpetrator used an administrative password, and the fact that Fandotech, the company that was hosting and managing the site, was not following correct web security procedures.

Information Source: Databreaches.net	*records from this breach used in our total: 18,059*

December 31, 2010	**Armstrong Atlantic State University** **Savannah, Georgia**	EDU	PORT	Unknown

Affected individuals may call (912) 344-3529.

A portable hard drive was stolen from the nursing department in early October. It contained the Social Security numbers of several hundred alumni.

Information Source: Databreaches.net	*records from this breach used in our total: 0*

December 20, 2010	**Saint Louis University** **St. Louis, Missouri**	EDU	HACK	Unknown

St. Louis University's network was breached during the week. At least some Social Security numbers and personal information of employees were exposed, but students also received notification of the breach. Employees who had been with the University for at least five years were affected.

Information Source: Databreaches.net	*records from this breach used in our total: 0*

December 19, 2010	**Stony Brook University** **Stony Brook, New York**	EDU	DISC	61,001 (No SSNs or financial

information
reported)

Student and faculty network and student IDs were posted online on sbuchat.com. A file with all registered student and faculty ID numbers could be downloaded in a PDF or Excel format. A systems engineer undergraduate discovered a flaw in the SOLAR system that allowed him to change students' NetID passwords without knowledge of the original password. The student then accessed the complete list of student and faculty IDs and posted the information.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| December 15, 2010 | **Ohio State University Columbus, Ohio** | EDU | HACK | 750,000 (Unknown numbers of SSNs and financial information) |

Affected individuals can find more information at www.osu.edu/creditsafety (www.osu.edu/creditsafety)

Students, professors and other University affiliates were notified that their information may have been accessed by a hacker. University officials discovered the breach in late October. Unauthorized individuals logged into an Ohio State server and had access to names, Social Security numbers, dates of birth and addresses of current and former students, faculty, staff, University consultants and University contractors.

UPDATE (1/14/11): 517,729 former students and 65,663 current students were affected. Exact numbers for current and former faculty, staff, consultants and contractors were not given.

UPDATE (2/22/2011): As of February 22, OSU was still attempting to find and inform affected individuals of the breach. Around 226,000 notification letters were mailed to alumni in February.

Information Source:
Databreaches.net

records from this breach used in our total: 750,000

| December 11, 2010 | **Kaplan University Chicago, Illinois** | EDU | INSD | Unknown |

The former dean of law and legal studies was convicted of making threats to students, staff and executives via email. The former University employee hacked into a colleague's email account and sent threats about identity theft and more to people during 2007. The former employee claims he was framed after threatening to expose the University's misconduct.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| December 10, 2010 | **University of Wisconsin - Madison Madison, Wisconsin** | EDU | HACK | 60,000 |

Some records of people affiliated with UW Madison were hacked into. The University discovered the breach on October 26 and sent notification to many former students, faculty and staff on November 30. One of the files had the photo ID of former students with their Social Security numbers embedded in the ID numbers and cardholder names. Only students enrolled prior to 2008 would have had their Social Security numbers exposed. It is unclear how far back the records date.

Information Source:
Databreaches.net

records from this breach used in our total: 60,000

| December 9, 2010 | **Methodist Theological School in Ohio**
Delaware, Ohio | EDU | PORT | Unknown |

The October 13 theft of a laptop resulted in the exposure of personal information of some people with a connection to MTSO. Names, Social Security numbers, dates of birth, financial payments received and letter grades for completed courses may have been stored on the laptop. The laptop was stolen from a locked off-campus site.

Information Source:
Databreaches.net   *records from this breach used in our total: 0*

| December 6, 2010 | **Dartmouth College**
Hanover, New Hampshire | EDU | PORT | 147 |

A stolen storage device contained the credit information of 147 parents and freshmen. The device was stolen from a secure room on November 8. Phone numbers, credit card numbers and credit card expiration dates for participants in the Dartmouth Outdoor Club First Year Program were on the device.

Information Source:
Databreaches.net   *records from this breach used in our total: 147*

| December 2, 2010 | **University of Arizona**
Tucson, Arizona | EDU | PORT | 8,300 |

An external hard drive was discovered to be missing from a secure records room. It was lost sometime in October or earlier. The hard drive contained former student withdrawal and disciplinary action records. Some Social Security numbers may have also been exposed. The relocation of the records room is one possible cause of the loss.

Information Source:
Databreaches.net   *records from this breach used in our total: 8,300*

| November 16, 2010 | **Messiah College**
Grantham, Pennsylvania | EDU | PORT | 43,000 |

An external hard drive was lost or stolen. Current, former and prospective students and their parents may have had their names, Social Security numbers, dates of birth and transcripts exposed. The information was from the financial aid department and spans from 1994 to 2010. Social Security numbers were not collected for all individuals involved, but exact number of individuals who had their Social Security or financial information exposed was not given.

UPDATE (11/21/10): The drive was found by the employee responsible for it. The likelihood that someone was able to access the information on the drive for a malicious purpose is very low or nonexistent.

Information Source:
Databreaches.net   *records from this breach used in our total: 43,000*

| November 7, 2010 | **Richmond Public Schools**
Richmond, Virginia | EDU | DISC | 110 |

An employee accidentally sent an email with the names, Social Security numbers and other personal information of 110 employees to 3,300 employees. Administrators began limiting access to the document and the entire email system after the mistake was discovered half an hour later. The email contained personnel changes, but was supposed to be emailed without the personal information of those employees who were moving within the organization.

Information Source:
Databreaches.net   *records from this breach used in our total: 110*

| November 2, 2010 | **Seton Hall University**
South Orange, New Jersey | EDU | DISC | 1,500 (No SSNs or financial information reported) |

An Excel spreadsheet with academic information was accidentally emailed to 400 students. Fifteen hundred students had their names, addresses, emails, student ID numbers, majors, credit hours and GPAs exposed. Students who received the attachment were instructed not to view or distribute it. Students were also informed to meet with the associate dean for Undergraduate Student Services and Enrollment Management if they had already opened the attachment.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| October 29, 2010 | **University of Hawai'i West O'ahu (UHWO)**
Pearl City, Hawaii | EDU | DISC | 40,101 |

Students from the University of Mānoa were also affected.

Unencrypted files that were placed on the faculty web server exposed student information. Student names, Social Security numbers, birth dates, addresses and academic information were placed on the server in December of 2009. Students who attended UHWO in Fall of 1994 or graduated between 1988 and 1993 were affected. A much larger number of students who attended the University of Hawai'i Mānoa between 1990 and 1998 were also affected. The files were removed on October 18 after a privacy group notified the University. The server was quickly removed from the network. The faculty member who accidentally placed the file on the server retired before the breach was discovered.

UPDATE (11/19/10): A former student is filing a class-action lawsuit on behalf of students affected by the University of Hawaii's multiple breaches. The man attended the Mānoa campus between 1990 and 1998 and claims that he was affected by the this breach and one that occurred in June of 2009. The names of four other people are attached to his Social Security number and his credit has been used in Georgia. Around 259,000 private records have been exposed by the University of Hawai'i since 2005.

UPDATE (1/27/2012): The University of Hawaii will provide two years of credit protection services and credit restoration services to settle a class-action lawsuit involving data breaches that affected nearly 100,000 students, faculty, alumni, and staff between 2009 and 2011. The settlement is still subject to court approval.

Information Source:
Databreaches.net

records from this breach used in our total: 40,101

| October 28, 2010 | **University of Connecticut Storrs**
Storrs Mansfield, Connecticut | EDU | DISC | 23 |

Student information from a class held in 2000 was discovered online. A faculty member had saved a list of one-time students in the class. The list exposed names and Social Security numbers and was removed from the Internet shortly after the discovery on October 4.

Information Source:
Databreaches.net

records from this breach used in our total: 23

| October 27, 2010 | **Houston Independent School District (HISD)**
Houston, Texas | EDU | HACK | 232,000 (30,000 employees) |

The HISD may have experienced a hacking incident over the weekend of October 24. Employees and students were unable to access the Internet, online classes and email until late Tuesday afternoon. Payroll information of workers and academic information of students may have been compromised along with other personal information.

UPDATE (12/2/10): HISD announced an overhaul of the computer system following the breach. Private employee, vendor and student data dating back 10 years could have been accessed by the hacker. Investigators have determined that the private data of one HISD student was viewed by the hacker. The investigation is ongoing.

Information Source: Databreaches.net   *records from this breach used in our total: 30,000*

| October 17, 2010 | **New Mexico Tech Community College** **Socorro, New Mexico** | EDU | DISC | 3,000 |

It appears that anyone with a Tech computer account could have accessed more than 3,000 Social Security numbers over the past four or five years. Copies of an accounting file were mistakenly stored in two public locations on the TCC server.

Information Source: Databreaches.net   *records from this breach used in our total: 3,000*

| October 15, 2010 | **University of North Florida** **Jacksonville, Florida** | EDU | HACK | 106,884 (52,853 SSNs reported) |

A hacker from outside of the country may have accessed applicant information sometime between September 24 and September 29. The information was mostly recruiting information and may have involved names, ACT and SAT scores, dates of birth and Social Security numbers.

Information Source: Databreaches.net   *records from this breach used in our total: 52,853*

| September 29, 2010 | **University of Florida** **Gainesville, Florida** | EDU | DISC | 239 |

People who believe they may have been affected may read the information provided on the University's privacy website at http://privacy.ufl.edu/ (http://privacy.ufl.edu/) . The University also has a toll-free privacy line 1-866-876-HIPA.

The University notified former students who took certain computer science classes in 2003 that their information was available online. Names, Social Security numbers and addresses were included in a web-accessible archive created by a faculty member. The University corrected the problem in August of 2010. Notification letters were sent to most students who may have been affected, but the University was unable to contact 54 former students.

Information Source: Databreaches.net   *records from this breach used in our total: 239*

| September 28, 2010 | **Maine Department of Education** **Augusta, Maine** | EDU | DISC | Unknown |

A technology director from the school district was able to access Social Security numbers of staff members in other districts. The Maine Department of Education has asked school districts to delay submitting student Social Security numbers until the problem has been addressed. According to reports, "For the first time, Maine school districts are collecting students' SSNs for a statewide database intended to help policy makers track students' progress throughout school and college and into the workplace." This practice has been controversial.

Information Source: Databreaches.net   *records from this breach used in our total: 0*

| September 17, 2010 | **Saint Anselm College** **Manchester, New Hampshire** | EDU | DISC | Unknown |

A number of alumni who received a University newsletter were notified that their Social Security numbers were printed on mailing labels. The error occurred on the spring 2010 and fall 2009 newsletters. It seems that no one complained about the fall accidental disclosure.

Information Source: Databreaches.net

records from this breach used in our total: 0

September 14, 2010	**Rice University Houston, Texas**	EDU	PORT	7,250 (4,003 Social Security numbers)

A portable device with personal information of current and former employees and some students was stolen. The device had a payroll file which contained the information of students, faculty, and staff on payroll as of January 2010. Social Security numbers, addresses, names, dates of birth and other employment information may have been exposed.

UPDATE (9/18/10): Additionally details reveal that the information was not encrypted. Approximately 2,270 students were affected. Four thousand of the Social Security numbers on the device were from faculty or staff, while three were from students. The banking information of two employees was also on the device.

Information Source: Databreaches.net

records from this breach used in our total: 4,003

September 11, 2010	**Corona-Norco Unified School District Norco, California**	EDU	DISC	82

An information privacy watchdog notified administrators that teacher and administrator personal information was available online. Most of the information was immediately removed, but a Google document with Social Security numbers was not removed. It is unknown how long the information was online, but it was discovered on August 31.

Information Source: Dataloss DB

records from this breach used in our total: 82

September 7, 2010	**City University of New York New York, New York**	EDU	PORT	7,000

Those with questions may call (212) 650-5426.

A computer with student information was stolen. The information included Social Security numbers and names.

Information Source: Dataloss DB

records from this breach used in our total: 7,000

September 5, 2010	**Eastern Michigan University Ypsilanti, Michigan**	EDU	HACK	Unknown

Online banking information may have been exposed because of a computer server hacking incident. The information included log-ins and personal identification numbers for some employees.

Information Source: Dataloss DB

records from this breach used in our total: 0

September 2, 2010	**Arkansas State University Jonesboro, Arkansas**	EDU	DISC	2,484

The full names, driver's license numbers and Social Security numbers of 2,484 full and part-time employees of the University were accidentally emailed to 144 University emails.

Information Source:
Databreaches.net

records from this breach used in our total: 2,484

| August 31, 2010 | **P.K. Yonge** **Gainesville, Florida** | EDU | PORT | 8,300 |

The July 23 theft of a laptop in California resulted in the exposure of current and former student and employee personal information. The information included Social Security numbers and some driver's license numbers. The information dates back to 2000.

Information Source:
Databreaches.net

records from this breach used in our total: 8,300

| August 24, 2010 | **Riverview Gardens School District** **St. Louis, Missouri** | EDU | PHYS | Unknown |

Hundreds of documents with student Social Security numbers, pictures, phone numbers and ages were left near a dumpster.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| August 20, 2010 | **University of Kentucky Newborn Screening Program** **Lexington, Kentucky** | EDU | PORT | 2,027 |

A laptop with information from the Department of Pediatrics Newborn Screening Program was stolen from a locked private office. Patient dates of birth, names and medical record numbers were on the password-protected laptop. Some patients also had Social Security numbers on the laptop.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 2,027

| August 19, 2010 | **University of Connecticut West Hartford** **West Hartford, Connecticut** | EDU | PORT | 10,174 |

The August 3 office theft of a laptop resulted in the exposure of 10,174 applicants' names, contact information and Social Security numbers. Undergraduate application information from 2004 to July of 2010 could have been accessed through the laptop.

Information Source:
Databreaches.net

records from this breach used in our total: 10,174

| August 12, 2010 | **Loma Linda University School of Dentistry** **Loma Linda, California** | EDU | STAT | 10,100 |

On the weekend of June 12, thieves stole three desktop computers with password protection. The computers did not contain patient treatment records, but did have Social Security numbers, dates of birth and other health information.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 10,100

| August 9, 2010 | **University of North Carolina at Greensboro** **Greensboro, North Carolina** | EDU | HACK | 2,300 |

In June, it was discovered that a University computer from the Speech and Hearing Center was infected with malware. Around 2,300 people who received services as far back as 1997 may have had their Social Security numbers, addresses, dates of birth, telephone numbers, insurance companies, and insurance ID numbers exposed. Another computer from the Psychology Clinic was discovered to have a similar problem. Around 240 people were affected; though no Social Security numbers or financial accounts were involved.

Information Source:
Dataloss DB

records from this breach used in our total: 2,300

July 29, 2010	**University of Virginia** **Charlottesville, Virginia**	EDU	PORT	Unknown

A transient was ordered to spend time in a men's diversion program after pleading guilty to stealing credit cards and electronics. One of the laptops he stole was a University-owned laptop. The man served 12 months in jail before being sentenced and slept in his car and in the University library during the time of the thefts.

Information Source:
Databreaches.net

records from this breach used in our total: 0

July 24, 2010	**University of Texas Arlington** **Arlington, Texas**	EDU	HACK	27,000 (2,048 SSNs reported)

Student records dating from 2000 to June 21, 2010 were compromised on a University file server on four separate occasions within the last two years. The server contained student health center prescription records.

Information Source:
Databreaches.net

records from this breach used in our total: 2,048

July 23, 2010	**Thomas Jefferson University Hospitals** **Philadelphia, Pennsylvania**	EDU	PORT	21,000

A password-protected laptop was stolen from the office of an employee on June 14. The computer should not have contained protected health information, but did. It also contained the name, birth date, gender, ethnicity, diagnosis, Social Security number, insurance information, and hospital account number of approximately 24,000 patients.

Information Source:
Databreaches.net

records from this breach used in our total: 21,000

July 23, 2010	**University of California San Francisco (UCSF) Medical Center** **San Francisco, California**	EDU	INSD	Unknown

A former employee used the Social Security numbers of his colleagues to obtain vouchers for Amazon.com purchases. He secretly used the Social Security numbers to create hundreds of accounts and complete 382 online StayWell health surveys in exchange for $100 online vouchers.

UPDATE (10/28/10): The former employee pled guilty to wire fraud and improper use of Social Security numbers. He was sentenced to 12 one year and one day in prison.

Information Source:
Databreaches.net

records from this breach used in our total: 0

July 16, 2010	**Buena Vista University**			

Storm Lake, Iowa	EDU	HACK	93,000

Someone gained unauthorized access to a BVU database. The database contained records of names, Social Security numbers, and driver's license numbers of BVU applicants, current and former students, parents, current and former faculty and staff, alumni and donors. These records go back as far as 1987.

Information Source:
Databreaches.net

records from this breach used in our total: 93,000

July 14, 2010	**Oregon State University** **Corvallis, Oregon**	EDU	HACK	34,000 (unknown number of SSNs)

A University computer containing personal information of current and former employees was found to be infected by a virus. Employee records from 1999 to 2005 contained Social Security numbers.

Information Source:
Databreaches.net

records from this breach used in our total: 0

July 14, 2010	**University of Pittsburgh Student Health Services** **Pittsburgh, Pennsylvania**	EDU	INSD	8,000 (Not included because no specific type of financial information stated)

An employee dishonestly took documents containing names and financial information. The employee was fired.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 0

July 7, 2010	**University of Hawai'i** **Honolulu, Hawaii**	EDU	STAT	53,000

53,000 people may have had their personal information exposed after a breach to the University of Hawai'i computer system was discovered. The university released statement that more than 40,000 Social Security numbers and 200 credit card numbers were part of the exposed information that was housed on a computer server used by the Mānoa campus parking office.

Information Source:
Dataloss DB

records from this breach used in our total: 53,000

July 6, 2010	**University of Florida** **Gainesville, Florida**	EDU	PHYS	2,047

Social Security numbers or Medicaid identification numbers were shared with a telephone survey company and included on address labels sent out to request research participation. The letters were sent through the U.S. Postal Service on May 24th and the issue was discovered on June 6th.

Information Source:
PHIPrivacy.net

records from this breach used in our total: 2,047

| June 29, 2010 | **University of Oklahoma** **Norman, Oklahoma** | EDU | HACK | Unknown |

The university's Information Technology department noticed unusual Internet activity on a laptop computer associated with its network. It determined the computer belonged to an employee and was infected with a virus known as Zeus or Z-Bod. The employee's laptop had access to computer files that contain student names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| June 29, 2010 | **University of Maine** **Orono, Maine** | EDU | HACK | 4,585 |

Hackers compromised the personal information of 4,585 students who received services from the school's counseling center. The center provides students with support and mental health services. The information on the servers included names, Social Security numbers and clinical information on every student who sought counseling services from the center between August 8, 2002 and June 21 of this year.

Information Source:
Dataloss DB

records from this breach used in our total: 4,585

| June 29, 2010 | **Cal State San Bernardino (CSSB)** **San Bernardino, California** | EDU | DISC | 36 |

Information such as names and Social Security numbers was exposed to the public through a web server. The students affected were on the class roster for a computer science and engineering course. The files were discovered and removed on June 10th.

Information Source:
Databreaches.net

records from this breach used in our total: 36

| June 29, 2010 | **Brooklyn Tech High School** **Brooklyn, New York** | EDU | HACK | 2,416; 103 Social Security numbers |

Hackers accessed PSAT information from the school and posted the names, home addresses, citizenship status, and Social Security numbers of students. The information was discovered on the school's website.

Information Source:
Databreaches.net

records from this breach used in our total: 103

| June 29, 2010 | **Ridgefield High School** **Ridgefield, Connecticut** | EDU | HACK | Unknown (the students of a few teachers) |

Two students were arrested for hacking into their school's computer system. Their goal appears to be changing their own grades; but they had access to the grades and personal information of other students.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| June 23, 2010 | **Florida International University** **Miami, Florida** | EDU | DISC | 19,495 |

Florida International University is in the process of sending notification letters to 19,407 students and 88 faculty members after the university's IT Security Office discovered personal data may have been exposed over the internet via a database's external search function. An announcement posted on the FIU website lists the personal data as GPAs, test scores, and Social Security numbers that were stored on the College of Education's E-Folio software app. This database kept track of student data related to state mastery standards, grade tracking, assignments, and Social Security numbers for both students and faculty.

Information Source:
Dataloss DB

records from this breach used in our total: 19,495

| June 18, 2010 | **University of Nevada**
Reno, Nevada | EDU | STAT | 7,526 |

Some patient information from the University Health System may have been accessed after the theft of computer equipment at the Reno office on June 11th. Patient names, Social Security numbers, patient account numbers, medical information, birth dates and addresses may have been viewed.

Information Source:
Databreaches.net

records from this breach used in our total: 7,526

| June 17, 2010 | **Ocean Lakes High School**
Virgina Beach, Virginia | EDU | HACK | 11,388 |

Schools that may have been accessed: Advanced Technology Center, Corporate Landing Middle School, Creeds Elementary School, Fairfield Elementary School, Indian Lakes Elementary School, Kellam High School, Kingston Elementary School, Landstown Middle School, Linkhorn Park Elementary School, Lynnhaven Middle School, New Castle Elementary School, Ocean Lakes Elementary School, Ocean Lakes High School, Red Mill Elementary School, Renaissance Academy, Rosemont Elementary School, Salem Elementary School, Technical & Career Education Center, Thalia Elementary School, Three Oaks Elementary School, Windsor Oaks Elementary School.

Over 11,388 students from schools listed on the Virginia Beach City County Public Schools page of publicschoolreview.com

Because of an incorrect security setting, an Ocean Lakes High School student was able to access a temporary file on a server that contained the names, addresses and Social Security numbers of students at 22 schools. The breach was discovered when the student tried to print some of the information in the school library. In addition to names, addresses and Social Security numbers, the student files also contain parent names, phone numbers, class schedules, birth dates and student ID numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 11,388

| June 7, 2010 | **New York City Department of Education**
New York, New York | EDU | HACK | Unknown |

The New York City's Special Commissioner Office revealed a hacker stole more than $640,000 from the Department of Education's petty cash account at JP Morgan Chase and distributed the codes to others to use to pay for student loans, gas bills and other purchases. The hacker allowed individuals to pay personal bills through EFTs and, in turn, he was given cash. The scam was discovered when an unidentified woman informed Chase someone was trying to pay bills using the account.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| June 3, 2010 | **Penn State**
University Park, Pennsylvania | EDU | DISC | 15,806,
25,000 more
later
discovered |

The Pennsylvania State University sent data breach notification letters to 15 806 individuals who at one time had their personal information,

including Social Security numbers, stored in a university database. Penn State issued a press release statement on Wednesday informing the university community that a computer in its Outreach Market Research and Data office was found to be actively communicating with a botnet CNC. According to the statement, the database used by the office had previously contained Social Security numbers on individuals. The university, which discontinued use of SSNs for identification purposes in 2005, nevertheless found that an archived copy of the information went undetected in the computer's cache.

UPDATE (6/8/10): An additional 25,000 individuals may have been affected.

Information Source:
Dataloss DB

records from this breach used in our total: 40,806

| June 2, 2010 | **Roanoke City Public Schools**
Roanoke, Virginia | EDU | PORT | 2000 |

Personal information of more than 2,000 Roanoke City Public Schools employees may be at risk. School officials said the hard drives of eight computers were not removed before the units were sold as surplus. "We believe that we have recovered all of the hard drives," said Superintendent Rita Bishop. The drives contained the names, school locations and Social Security numbers of the division's employees as of November 2006. The division will be setting up a hotline for employees to call with questions and concerns. Free credit monitoring service will be offered to affected employees.

Information Source:
Dataloss DB

records from this breach used in our total: 2,000

| June 2, 2010 | **University of Louisville**
Louisville, Kentucky | EDU | DISC | 709 |

A University of Louisville database of 708 names that included Social Security numbers and dialysis details was available on the Internet without password protection for nearly a year and a half. The Web site was disabled on May 17 when the university discovered the flaw. University officials said in a statement that accessing the database would not have been easy, and no direct links to the database were discovered. The information was available so long because the U of L doctor who set up the Web site thought the information was protected by a password and other precautions. U of L was finally notified when someone outside the university sent an e-mail about open access to the information. The Web site was shut down an hour later.

Information Source:
Dataloss DB

records from this breach used in our total: 709

| May 24, 2010 | **Lake Ridge Middle School**
Woodbridge, Virginia | EDU | PORT | 1,200 (0 SSNs reported) |

A USB drive containing student names, identification numbers, phone numbers, and medical information was stolen from the unlocked car of a school administrator at the employee's home. Over 1,200 students were affected.

Information Source:
Databreaches.net

records from this breach used in our total: 0

| May 21, 2010 | **Tufts University**
Medford, Massachusetts | EDU | HACK | 2,000 |

Campus computers with former student files were exposed to a virus. Over two thousand alumni may have had their Social Security numbers and other information exposed.

Information Source:
Databreaches.net

records from this breach used in our total: 2,000

| May 17, 2010 | **Edward Waters College**
Jacksonville, Florida | EDU | DISC | 210 |

Over 210 staff and prospective student names, Social Security numbers, driver's license numbers, and addresses were accessible to the public through a Google or Yahoo! search. The cause was a mistake in setting up software.

Information Source:
Databreaches.net

records from this breach used in our total: 210

| April 28, 2010 | **Montana Tech**
Butte, Montana | EDU | DISC | 260 |

A Montana Tech employee mistakenly included the personal information of former students in an e-mail message sent to faculty, staff and students last week. The e-mail was an invitation to watch students present their research projects. But the file that this year's information was taken from included the names, addresses, Social Security numbers and in some cases birth dates of students whose research projects were done from 1998 through 2005.

Information Source:
Dataloss DB

records from this breach used in our total: 260

| April 23, 2010 | **Chattanooga State**
Chattanooga, Tennessee | EDU | PHYS | 1,700 |

Nearly two thousand students records from Chattanooga State are missing. The company hired to scan the documents, mishandled them. The school took the records to a company, United Imaging in Walker County, where the papers would be converted to computer discs. The school was contacted by individuals who said there was something awry going on at this scanning site. That's when the school found their records in disarray, and brought them back. The papers included students' names, Social Security numbers, addresses, phone numbers, some even contained high school transcripts. Chattanooga State went through each item, hand by hand, and found nearly 2000 missing documents from 2007.

Information Source:
Dataloss DB

records from this breach used in our total: 1,700

| March 30, 2010 | **Three Rivers Community College**
Norwich, Connecticut | EDU | HACK | Unknown |

Three Rivers Community College may have suffered a security breach due to unauthorized access to its computer network. Data made vulnerable in the breach included names and Social Security numbers. Those affected would have been involved in the following programs during these years:
1997-2009: Participants in the Real Estate programs
2004-2009: Participants in the Life Long Learners programs
2003-2006: Participants in the Patient Care Technicians programs
2004-2006: Participants in the Certified Nursing Assistant programs
2004-2005: Participants in the Electric Boat academic programs
2007-2008: Participants in the Bridges to Health Care Careers programs
2006-2008: Participants in the Photons for Educators programs
2004-2009: Faculty or staff members of the Three Rivers Continuing Education office.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| March 25, 2010 | **Evergreen Public Schools**
Vancouver, Washington | EDU | INSD | 5,000 |

A 21-year-old former Evergreen Public Schools student has pleaded guilty to criminal charges in connection with a computerized payroll security breach that put more than 5,000 past and current Vancouver district school employees at risk of identity theft. The man had

"shoulder-surfed" a password from an Evergreen school employee while still a student there.

Information Source: Dataloss DB

records from this breach used in our total: 5,000

| March 25, 2010 | **Valencia High School**
Valencia, California | EDU | INSD | Unknown |

A student gained access to the entire district of Hart's system, but only went into his high school's portion. The student claimed he changed some things and then returned them. The student most likely used a password, but it is not known whether he used a district computer or a personal one. The district is providing one year of free credit monitoring services.

Information Source: Databreaches.net

records from this breach used in our total: 0

| March 25, 2010 | **Johns Hopkins University School of Education**
Baltimore, Maryland | EDU | DISC | Unknown |

A file containing student enrollment information was accessible online. Student names, races, genders, Social Security numbers, identification numbers and dates of birth were accessible for at least one month.

Information Source: Databreaches.net

records from this breach used in our total: 0

| March 18, 2010 | **Vanderbilt University**
Nashville, Tennessee | EDU | STAT | 7,174 |

A professor's desktop computer, containing the names and Social Security numbers of 7,174 current and former students was stolen some time during the weekend of Feb. 6.

Information Source: Dataloss DB

records from this breach used in our total: 7,174

| March 18, 2010 | **California State University, Los Angeles (Cal State Los Angeles)**
Los Angeles, California | EDU | STAT | 232 |

Cal State Los Angeles has notified 232 former students that a computer stolen from the mathematics department office last month may have contained personal information such as their Social Security numbers and grades.

Information Source: Dataloss DB

records from this breach used in our total: 232

| March 11, 2010 | **Bennett College**
Greensboro, North Carolina | EDU | HACK | 1,100 |

A payroll computer was breached. Names, Social Security numbers, birth dates, pay rates, and bank transit numbers were exposed.

Information Source: Databreaches.net

records from this breach used in our total: 1,100

| March 10, 2010 | **Wickenburg Unified School District**
Wickenburg, Arizona | EDU | DISC | 1,438 |

State auditors found that the District's network was accessible to unauthorized users. Backup servers were kept in an easily accessible room. Names, Social Security numbers, addresses and birth dates of students were left exposed.

Information Source: Databreaches.net

records from this breach used in our total: 1,438

| February 19, 2010 | **Valdosta State University**
Valdosta, Georgia | EDU | HACK | 170,000 |

http://www.valdosta.edu/notify/ (http://www.valdosta.edu/notify/)

A Valdosta State server that was reported as being breached could have exposed the information of up to 170,000 students and faculty. Valdosta State officials reported the discovery of a breach on Dec. 11 and estimated it began on Nov. 11. The university said the grades and Social Security numbers of up to 170,000 students and faculty were exposed in the breach.

Information Source: Dataloss DB

records from this breach used in our total: 170,000

| February 17, 2010 | **Southern Illinois University**
Carbondale, Illinois | EDU | HACK | 900 |

A computer security breach at Southern Illinois University may have put hundreds of alumni at risk of identity theft. A faculty member's computer in the Mathematics Department was found to be infected with malicious software. When the computer files were searched, university officials discovered there were Social Security numbers for approximately 900 students who took introductory math classes at SIU in 2004 and 2005 stored on the hard drive.

Information Source: Dataloss DB

records from this breach used in our total: 900

| February 9, 2010 | **Kansas City Art Institute**
Kansas City, Kansas | EDU | STAT | 145 |

About 145 employees at the Kansas City Art Institute have been notified of potential identity theft in connection with the disappearance of a computer from the campus. An Apple computer that contained Social Security numbers, dates of birth and other personal information about the school's professors and staff employees was stolen from the human resource office.

Information Source: Dataloss DB

records from this breach used in our total: 145

| February 6, 2010 | **University of Texas, El Paso**
El Paso, Texas | EDU | DISC | 15,000 |

University of Texas at El Paso is notifying students that their Social Security numbers were visible when their tax forms were sent out. The University notified 15,000 students but they don't know exactly how many students were affected. UTEP blames a glitch in a machine used to fold letters when student's forms were sent out. Some of the forms were folded in such a way that the document shifted on the envelope and allowed for the Social Security numbers to be visible through the mailing window on the envelope.

Information Source: Dataloss DB

records from this breach used in our total: 15,000

| February 1, 2010 | **West Virginia University**
Morgantown, West Virginia | EDU | DISC | 53 |

Around 53 West Virginia University students' personal information was available to others following an "operational error" during a routine update of tax information. The students' 1098-T forms, which include their Social Security number and tax identification numbers, among others, were uploaded to the University's 1098-T Web site. The forms are distributed to WVU students who are U.S. citizens who paid tuition during the 2009 calendar year. They can be used to claim federal tax credit. Students can typically access their forms on the site for tax purposes, but the error made the information viewable to any WVU student on the site.

Information

Source:
Dataloss DB

records from this breach used in our total: 53

| January 28, 2010 | **Humboldt State University**
Arcata, California | EDU | HACK | 3,500 |

A Humboldt State University computer infected with a virus may have exposed the personal information of 3,500 people employed by the school between 2002 and 2006. The computer was found to have a sophisticated virus that is used to steal login information.

Information
Source:
Dataloss DB

records from this breach used in our total: 3,500

| January 21, 2010 | **University of Missouri System**
Columbia, Missouri | EDU | DISC | 75,000 |

About 100 people responded to an e-mail notifying students that their Social Security numbers may have been visible in the envelope window of a tax form sent by the University of Missouri System. More than 75,000 Form 1098-Ts were mailed. The four-campus system has no way of assessing how many envelopes displayed the numbers. Form 1098-T is an Internal Revenue Service form that reports tuition billed and paid. Campus Mail Services committed the folding errors.

Information
Source:
Dataloss DB

records from this breach used in our total: 75,000

| January 6, 2010 | **Eugene School District**
Eugene, Oregon | EDU | HACK | 13,000 |

Email databreach@4j.lane.edu (mailto:databreach@4j.lane.edu) or call (541) 790-7730 for more information.

Hackers breached the security of a computer server containing the names, phone numbers and employee ID numbers of current and former Eugene School District employees. The server in question did not contain other personal information but was attached to servers that contain Social Security numbers and other sensitive data. It is possible that the individuals responsible may have accessed names, addresses, dates of birth, Social Security numbers, tax identification numbers and direct-deposit bank account information for current and former staff members.

Information
Source:
Dataloss DB

records from this breach used in our total: 13,000

| December 31, 2009 | **Eastern Washington University**
Cheney, Washington | EDU | HACK | 130,000 |

Eastern Washington University is trying to notify up to 130,000 current or former students whose names, Social Security numbers and dates of birth were on a computer network involved in a security breach. The student information goes back to 1987. The notification process could take up to two weeks. The University recently discovered the breach during an assessment of its network. Information-technology staff also discovered that the hacker installed software to store and share video files on the system.

Information
Source:
Dataloss DB

records from this breach used in our total: 130,000

| December 23, 2009 | **Penn State University**
University Park, Pennsylvania | EDU | HACK | 30,000 |

The University sent out letters notifying those potentially affected by malware infections, which are believed responsible for breaches. The areas and extent of the records involved in the malicious software attack included Eberly College of Science, 7,758 records; the College of Health and Human Development, 6,827 records; and one of Penn State's campuses outside of University Park, approximately 15,000 records.

Information

Source: *records from this breach used in our total: 30,000*
Dataloss DB

| December 22,
2009 | **Western Michigan University**
Kalamazoo, Michigan | EDU | DISC | Unknown |

University officials discovered that student employee information was viewable online. The information included names, addresses and
Social Security numbers.

Information
Source: *records from this breach used in our total: 0*
Databreaches.net

| December 18,
2009 | **Dickinson School of Law**
Carlisle, Pennsylvania | EDU | HACK | 261 |

A computer in the Dickinson School of Law that contained 261 Social Security numbers from an archived class list was found to be infected
with malware that enabled it to communicate with an unauthorized computer outside the network.

Information
Source: *records from this breach used in our total: 261*
Dataloss DB

| December 17,
2009 | **North Carolina Libraries**
Raleigh, North Carolina | EDU | HACK | 51,000 |

Library users at 25 campuses were the victims of a security breach in August. The libraries collect driver's license and Social Security
numbers to help identify computer users. The information is stored on a central server in Raleigh. Other campuses affected are Alamance,
Beaufort, Bladen, Blue Ridge, Brunswick, Central Carolina, College of the Albemarle, Gaston, Halifax, Haywood, Lenoir, Martin, Nash,
Pamlico, Piedmont, Richmond, Roanoke-Chowan, Rowan-Cabarrus, Sandhills, Southwestern, Tri-County, Vance Granville and Wilson.

Information
Source: *records from this breach used in our total: 51,000*
Dataloss DB

| December 15,
2009 | **The Beijing Center for Chinese Studies**
Chicago, Illinois | EDU | PORT | Unknown |

(877) TBS-5060
http://www.thebeijingcenter.org/securityqns (http://www.thebeijingcenter.org/securityqns)

The theft of a laptop exposed applications for study abroad students. Names and Social Security numbers were exposed. An unknown
number of NH residents were affected.

Information
Source: *records from this breach used in our total: 0*
Dataloss DB

| December 10,
2009 | **Bushland Elementary School**
Bushland, Texas | EDU | PHYS | 100 |

A Potter County school district has improved security protecting its student records after paperwork containing Social Security numbers,
family incomes and student addresses was discovered at a recycling site in Canyon. The documents listed names of about 100 students at
Bushland Elementary School who were eligible for free or reduced-price meals through a federal program during the 2003-04 and 2005-06
school years. Applications for subsidized meals from more than 20 families included their Social Security numbers, incomes, addresses and
phone numbers.

Information

Source:
Dataloss DB

records from this breach used in our total: 100

December 7,
2009

**Gateway Community College
New Haven, Connecticut**

EDU   HACK   Unknown

The College attempted to notify potential victims of a breach caused by malware discovered on campus computers. College alumni who donated to the College, potential donors, and students receiving scholarships between 2004 and 2006 may have been affected.

Information Source:
Databreaches.net

records from this breach used in our total: 0

December 5,
2009

**Wake County Schools
Raleigh, North Carolina**

EDU   DISC   5,000

The Wake County school system accidentally sent out about 5,000 postcards with students' Social Security Numbers printed on the front. Wake schools mailed about 15,000 reminders asking parents to specify if they want to keep their children in magnet or traditional calendar schools. About a third of those cards had the Social Security Numbers printed alongside the child's name - a holdover from recent years when those nine-digit numbers were used to identify students.

Information Source:
Dataloss DB

records from this breach used in our total: 5,000

December 4,
2009

**Deo B. Colburn Foundation Scholarship
Lake Placid, New York**

EDU   DISC   341

If you received the Deo B. Colburn scholarship for the 2003-04 academic year, your Social Security number may have been made public. Hundreds of Social Security numbers of former students from all over the northern Adirondacks, including Lake Placid, were released onto the Internet, potentially compromising those people's credit and financial status. Information included names, addresses, academic institutions, the amount of money received and Social Security numbers of the scholarship recipients.

Information Source:
Dataloss DB

records from this breach used in our total: 341

December 4,
2009

**Eastern Illinois University
Charleston, Illinois**

EDU   HACK   9,000

A computer was compromised by a virus. It caused the University's Office of Admissions server to be infected with a number of viruses, including several that could allow an external person to access the server. The incident was discovered during a routine security check. The investigation later determined the breach extended to two other computers with personal data from student files or applications.

Information Source:
Dataloss DB

records from this breach used in our total: 9,000

December 4,
2009

**Eastern Illinois University
,**

EDU   HACK   9,000

A computer was compromised by a virus. That caused the University's Office of Admissions server to be infected with a number of viruses, including several that could allow an external person to access the server. The incident was discovered during a routine security check. The investigation later determined the breach extended to two other computers with personal data from student files or applications.

Information Source:
Dataloss DB

records from this breach used in our total: 9,000

December 4,

University of Nebraska

| 2009 | **Omaha, Nebraska** | EDU | HACK | 1,400 |

A computer in the College of Education and Human Sciences at the Lincoln campus was breached. The security breach was discovered last month at the University of Nebraska involving the names, addresses and Social Security Numbers of 1,400 Hinsdale High School District 86 graduates. The University's investigation revealed the computer had not been adequately secured, allowing unauthorized external access to the computer and its information.

Information Source:
Dataloss DB

records from this breach used in our total: 1,400

| November 26, 2009 | **Penn State**
University Park, Pennsylvania | EDU | HACK | 303 |

A Penn State professor's grade book from 2001 to 2004 that contained 303 students' Social Security numbers, among other personal information, was found to be compromised by a computer virus.

Information Source:
Dataloss DB

records from this breach used in our total: 303

| November 21, 2009 | **Notre Dame University**
Notre Dame, Indiana | EDU | DISC | Unknown |

Notre Dame is warning university employees to keep an eye on their bank accounts after a security breach. Personal information of some past and current employees - including name, Social Security number and birth date - was accidentally posted onto a public website. The error was corrected and the information removed from the website.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| November 6, 2009 | **Chaminade University**
Honolulu, Hawaii | EDU | DISC | 4,500 |

www.chaminade.edu/infosecure
(http://www.chaminade.edu/infosecure) infosecure@chaminade.edu

Chaminade University inadvertently posted confidential information, including Social Security numbers, of thousands of students, on its Web site for months. An investigation determined the report was placed on obscure -- though publicly accessible -- Web pages because of human error, according to a university news release. The information was accessible for about eight months, although there is no evidence of its use, officials said. The university estimates that personally identifiable data for 4,500 students were in the report. Those affected include undergraduate students who attended the university from 1997 to 2006.

Information Source:
Dataloss DB

records from this breach used in our total: 4,500

| October 21, 2009 | **Bullitt County Public Schools**
Shepherdsville, Kentucky | EDU | DISC | 676 |

A Bullitt County Public Schools employee accidentally sent an e-mail message to about 1,800 school district workers that included the names and Social Security numbers of 676 district employees. The employees were identified as not having completed the district's 2010 open-enrollment process for insurance, and the e-mail was intended as a reminder to complete the process.

Information Source:
Dataloss DB

records from this breach used in our total: 676

| October 21, 2009 | **Roane State Community College**
Harriman, Tennessee | EDU | PORT | 14,783 |

Hotline (865) 882-4688, (866) 462-7722 ext. 4688

Roane State Community College has announced that the names and Social Security numbers of 9,747 current or former students were on a data storage device stolen from an employee's vehicle, along with 1,194 current/former employees' information. The Social Security numbers alone, with no names, were also stolen for 5,036 additional current or former students. The data was on a 4GB USB drive used for work-related purposes. An employee took it home to do work after hours, and left it in the car. The employee forgot to lock the car doors. The USB drive was stolen along with a personal hand-held device.

Information Source:
Dataloss DB

records from this breach used in our total: 14,783

| October 15, 2009 | **Virginia Department of Education**
Richmond, Virginia | EDU | PORT | 103,000 |

(877) 347-5224

A flash drive containing the personal information of more than 103,000 former adult education students in Virginia was misplaced. The information included names, Social Security numbers and employment and demographic information. The flash drive contained information on all students who finished an adult education course in Virginia from April 2007 through June 2009 or who passed a high school equivalency test between January 2001 and June 2009.

Information Source:
Dataloss DB

records from this breach used in our total: 103,000

| October 4, 2009 | **Suffolk Community College**
Selden, New York | EDU | DISC | 300 |

Suffolk Community College has agreed to pay a company for the next year to monitor the credit of 300 students whose last names and Social Security numbers were mistakenly listed in an attachment to an e-mail sent to those students last month.

Information Source:
Dataloss DB

records from this breach used in our total: 300

| September 25, 2009 | **University of North Carolina, Chapel Hill**
Chapel Hill, North Carolina | EDU | HACK | 236,000
(163,000 SSNs estimated) |

A hacker has infiltrated a computer server housing the personal data of 236,000 women enrolled in a UNC Chapel Hill research study. The Social Security numbers of 163,000 participants were among the information exposed. The data is part of the Carolina Mammography Registry, a 14-year-old project that compiles and analyzes mammography data submitted by radiologists across North Carolina.

UPDATE (10/6/10): A lead researcher at the University is fighting a demotion and pay cut that resulted from the data breach in the medical study she directs. It appears that the incident first occurred in 2007 and was not discovered until 2009. An attorney representing the researcher claims that his client is not at fault because the University knew that the program's computer system had security deficiencies in 2006. The University claims that the researcher acted negligently, but the attorney claims that the researcher was not alerted to the security flaws and there is no evidence that the researcher violated or ignored rules in obtaining patient information.

UPDATE (5/9/2011): The researcher and University reached a settlement. The researcher agreed to retire at the end of 2011 and will receive her full rank and salary until that time.

Information Source:
Dataloss DB

records from this breach used in our total: 163,000

September 23, 2009	**Eastern Kentucky University** **Richmond, Kentucky**	EDU	DISC	5,045

(859) 622-7777, ecert@eku.edu (mailto:ecert@eku.edu)

The names and Social Security numbers of about 5,000 Eastern Kentucky University faculty, staff and student workers were posted inadvertently on the Internet last September, where they have been displayed for a year.

Information Source:
Dataloss DB

records from this breach used in our total: 5,045

September 14, 2009	**University of Florida** **Gainesville, Florida**	EDU	DISC	25

(866) 876-HIPA (4472)

In August, the University's Privacy Office was notified of a privacy breach after the discovery of an unprotected computer file containing 34 names and 25 Social Security numbers. It's believed the personal information belongs to trainers working with the Florida Traffic and Bicycle Safety Education program in 2006. The file was immediately removed.

Information Source:
Dataloss DB

records from this breach used in our total: 25

September 7, 2009	**School for the Physical City High School** **New York, New York**	EDU	PHYS	Unknown

Boxes of student records were piled in the street in front of the old home of the School for the Physical City. Some records contained the Social Security numbers, grades, signatures and even psychological reports of former students of the public intermediate high school. The boxes contained hundreds of records and were sitting next to a trash bin filled with old desks and other discarded school supplies. The School for the Physical City moved to a new location over the summer and apparently the records were thrown out with the trash during the relocation.

UPDATE (9/12/10): A parent and child are suing the New York City Department of Education.

Information Source:
Dataloss DB

records from this breach used in our total: 0

September 2, 2009	**Bluegrass Community and Technical College** **Danville, Kentucky**	EDU	UNKN	100

A file containing the personal information including Social Security numbers of nearly 100 students at the Bluegrass Community and Technical College has been stolen.

Information Source:
Dataloss DB

records from this breach used in our total: 100

August 21, 2009	**University of Massachusetts** **Amherst, Massachusetts**	EDU	HACK	Unknown

Nearly a year ago, hackers broke into a computer server that contained Social Security numbers and a very limited amount of credit card information for graduates of University of Massachusetts. Hackers gained access to one server on the university's computer system, which held information of students who attended UMass between 1982 and 2002, as well as a few who attended before 1982. A UMass spokesman declined to say how many people's records were exposed, except that it was a large number of undergraduate and graduate students who attended the university during the 20-year period.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 0

| August 20, 2009 | **Cal State Los Angeles**
 Los Angeles, California | EDU | PORT | 600 |

(800) 883-4029

The theft of two desktop and 12 laptop computers from an office at Cal State Los Angeles is causing identity theft concerns for more than 600 students and faculty members. Someone broke a window in the office of the university's Minority Opportunities in Research program to steal the computer. The computers stolen contained individual names, Social Security numbers and addresses, according to campus.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 600

| August 15, 2009 | **Northern Kentucky University**
 Highland Heights, Kentucky | EDU | PORT | 200 |

A Northern Kentucky University employee's laptop computer - which contained personal information about some current and former students -- was stolen from a restricted area. The personal information stored on the employee's computer included Social Security numbers of at least 200 current and former students.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 200

| August 14, 2009 | **Calhoun Area Career Center**
 Battle Creek, Michigan | EDU | DISC | 455 |

Personal information from 455 students at Calhoun Area Career Center during the 2005-2006 school year was available online for more than three years. The information included names, Social Security numbers, 2006 addresses and telephone numbers, birth dates and school information. There were about 1,000 students at the career center during that time, but an investigation by the Calhoun County Intermediate School district found that information for 455 students was available.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 455

| August 11, 2009 | **University of California, Berkeley School of Journalism**
 Berkeley, California | EDU | HACK | 493 |

https://security.berkeley.edu/jschool-info (https://security.berkeley.edu/jschool-info)

Campus officials discovered during a computer security check that a hacker had gained access to the journalism school's primary Web server. The server contained much of the same material visible on the public face of the Web site. However, the server also contained a database with Social Security numbers and/or dates of birth belonging to 493 individuals who applied for admission to the journalism school between September 2007 and May 2009.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 493

| July 29, 2009 | **University of Colorado, Colorado Springs**
 Colorado Springs, Colorado | EDU | PORT | 766 |

The university is notifying nearly 800 students and alumni that some of their personal information may have been on a stolen laptop. That laptop was taken from a professor's home on July 5th after the home was burglarized. The laptop contained class roster information - name, student ID number, e-mail address, graduating class year and grade information - for current and past UCCS students. No financial

information was stored on the laptop, but there is a possibility that Social Security numbers may have been involved for students enrolled prior to summer, 2005.

Information Source:
Dataloss DB

records from this breach used in our total: 766

| July 17, 2009 | **Francis Howell School District**
 St. Charles, Missouri | EDU | PORT | 1,700 |

A laptop computer theft could have compromised personal information. The computer could have contained names and Social Security numbers for 1,700 non-certified employees. Anyone who worked for the district from 2005 through 2008 could be affected. The computer belonged to a Francis Howell employee in the district human resources department.

Information Source:
Dataloss DB

records from this breach used in our total: 1,700

| July 14, 2009 | **Canyons School District**
 Cottonwood Heights, Utah | EDU | PORT | 6,000 |

Canyons School District officials are investigating the disappearance of a thumb drive that contained the personal information of more than 6,000 current and recent employees. The USB flash drive is believed to have contained employee addresses, phone numbers, dates of birth and Social Security numbers. A district-level worker was using it to transfer data for apparently legitimate, job-related purposes.

Information Source:
Dataloss DB

records from this breach used in our total: 6,000

| July 14, 2009 | **Leander School District**
 Leander, Texas | EDU | UNKN | Unknown |

School officials sent a notice home with special needs students to alert parents that someone gained access to private information. It appears that one individual gained unauthorized electronic access to confidential information.

Information Source:
Media

records from this breach used in our total: 0

| June 26, 2009 | **University of Central Missouri Police Department (UCM)**
 Warrensburg, Missouri | EDU | INSD | 250 |

The University sent letters to 7,000 students, but the final number of affected individuals appears to be closer to 250

After two documents containing student personal information were stolen, it was discovered that a former University police officer and his wife were responsible. They used the names, Social Security numbers, and birth dates of students enrolled in 2005 and 2006 summer sessions. The thieves fraudulently opened bank accounts, received student loans, and applied for credit and debit cards. The losses total more than $30,000.

Information Source:
Databreaches.net

records from this breach used in our total: 250

| June 23, 2009 | **Cornell University**
 Ithaca, New York | EDU | PORT | 45,277 |

A stolen Cornell University computer has compromised the personal information of thousands of members of the University community. The computer contains the names and Social Security numbers of current and former students as well as current and former faculty and staff members.

Information Source: Dataloss DB		*records from this breach used in our total: 45,277*	

June 12, 2009	**Kirkwood Community College** **Cedar Rapids, Iowa**	EDU	PORT	1,600

Someone took a storage device from a counselor's office in Iowa City. That device contained names and Social Security numbers for participants in the PROMISE JOBS program.

Information Source: Dataloss DB		*records from this breach used in our total: 1,600*	

June 12, 2009	**Oregon Health & Science University** **Portland, Oregon**	EDU	PORT	4,000

A physician's laptop was stolen from a car parked at the doctor's home. Patient names, treatment dates, short medical treatment summaries and medical record numbers were stored on the computer. There were no home addresses, billing information or Social Security numbers stored on the laptop.

UPDATE (08/11/10): It seems that as many as 4,000 patients may have been affected and Social Security numbers were involved.

Information Source: Dataloss DB		*records from this breach used in our total: 4,000*	

June 6, 2009	**Ohio State Dining Services** **Columbus, Ohio**	EDU	DISC	350

Student employees had their Social Security numbers accidentally leaked in an e-mail. The hiring coordinator for Dining Services, an OSU student, received an e-mail with an attachment that included students' names and SSNs. He accidentally sent the attachment in an e-mail reminding student employees to sign their waivers for the Ohio Employees Retirement System. After realizing the mistake, the hiring coordinator called the Office of Information Technology, which stopped the e-mails before all of them were sent.

Information Source: Dataloss DB		*records from this breach used in our total: 350*	

June 5, 2009	**Virginia Commonwealth University** **Richmond, Virginia**	EDU	STAT	17,214

A desktop computer was stolen from a secured area within Cabell Library in mid-April. The computer may have contained student names, Social Security numbers and test scores dating from October 2005 to the present. VCU discontinued use of Social Security numbers as ID numbers in January 2007. An additional 22,500 students are being notified that their names and test scores may have also been on the computer. No Social Security numbers were recorded with those names, but computer-generated student ID numbers may have been.

Information Source: Dataloss DB		*records from this breach used in our total: 17,214*	

June 1, 2009	**University of Nevada - Las Vegas** **Las Vegas, Nevada**	EDU	HACK	20

A UNLV computer was compromised and may have allowed loss of some personal data. The College of Sciences recently sent a letter to about 20 students as officials became aware of a virus affecting a computer in the College. The College found no information was leaked, but for legal reasons they still sent the letter.

Information

Source:
Media

records from this breach used in our total: 20

| May 27, 2009 | **Warren County Virtual Community School**
Lebanon, Ohio | EDU | PHYS | 140 |

Contractors installing fiber on a near by street to the school say they found a four-page list in a recycling dumpster when they went to dump some trash. The list had more than 140 students' names, addresses, Social Security numbers and birth dates listed. Their parents names were on the list too.

Information
Source:
Dataloss DB

records from this breach used in our total: 140

| May 11, 2009 | **Office of the State Superintendent of Education D.C.**
Washington, District Of Columbia | EDU | DISC | 2,400 |

The D.C. agency that handles college financial aid requests had accidentally e-mailed personal information from 2,400 student applicants to more than 1,000 of those applicants. An employee of the agency's Higher Education Financial Services Program inadvertently attached an Excel spreadsheet to an e-mail. The information included student names, e-mail and home addresses, phone and Social Security numbers and dates of birth.

Information
Source:
Dataloss DB

records from this breach used in our total: 2,400

| May 7, 2009 | **University of California, Berkeley**
Berkeley, California | EDU | HACK | 160,000 |

http://datatheft.berkeley.edu (http://datatheft.berkeley.edu)

Hackers infiltrated restricted computer databases. Personal information of 160,000 current and former students and alumni may have been stolen. The University says Social Security numbers, health insurance information and non-treatment medical records dating back to 1999 were accessed. The breach was discovered April 21, 2009, when administrators performing routine maintenance identified messages left by the hackers. They found that restricted electronic databases had been illegally accessed by hackers beginning on October 9, 2008 and continued until April 6, 2009. All of the exposed databases were removed from service to prevent further attacks.

Information
Source:
Dataloss DB

records from this breach used in our total: 160,000

| May 4, 2009 | **Kapiolani Community College**
Honolulu, Hawaii | EDU | HACK | 15,487 |

More than 15,000 students at Kapiolani Community College are at risk of identity theft because of an Internet security breach. School officials found that a computer was infected with malware that can steal sensitive data. The computer contained the personal information of 15,487 students who applied for financial aid between January 2004 and April 15. The computer did not have sensitive information, but it was hooked up to a network that had access to names, addresses, phone numbers dates of birth and Social Security numbers.

Information
Source:
Dataloss DB

records from this breach used in our total: 15,487

| April 29, 2009 | **Orleans Parish Public Schools**
New Orleans, Louisiana | EDU | PHYS | Unknown |

The confidential records of Orleans Parish public-school employees have been discovered in an abandoned and unsecured warehouse in New Orleans. Personnel files, payroll records, and other documents with private data were uncovered. Inside were countless boxes filled with confidential information, not to mention stacks of other documents lying on the ground, listing payroll information, worker evaluations, notices of personnel action, and investigations into employee discrimination. Also found were full names, home addresses, and Social

Security numbers on document after document.

Information Source:
Media

records from this breach used in our total: 0

April 13, 2009   **Irving Independent School District**   EDU   PHYS   Unknown
                   Irving, Texas

Identity thieves using the names and Social Security numbers of Irving Independent School District employees have made thousands of dollars in credit card purchases. At least 64 of the 3,400 teachers and other employees names were on an old benefits report that somehow ended up in the trash.

UPDATE (2/4/10): At least one woman involved in the crime was caught in January of 2009 and sentenced on February 4, 2010.

Information Source:
Media

records from this breach used in our total: 0

April 9, 2009   **Penn State Erie/Behrend College**   EDU   HACK   10,868
                  Erie, Pennsylvania

On March 23, the University confirmed that 10,868 Social Security numbers in historical data on a computer at Penn State Erie, The Behrend College, could have been breached. Longstanding security measures, designed to protect the network and systems from malicious software, alerted the University to the potential breach. As soon as the University became aware of the malicious software on this computer, the computer was immediately taken off line, data was examined and information was removed.

Information Source:
Dataloss DB

records from this breach used in our total: 10,868

April 8, 2009   **Metro Nashville School/Public Consulting Group**   EDU   DISC   18,000
                  Nashville, Tennessee

(615) 259-INFO (4636)

Metro Nashville students' names, Social Security numbers, addresses and dates of birth and parents' demographic information were available by searching Google. A private contractor unintentionally put student data on a computer Web server that wasn't secure. The data was available online from Dec. 28 to March 31.

Information Source:
Dataloss DB

records from this breach used in our total: 18,000

March 27, 2009   **Pacific University**   EDU   PORT   Unknown
                   Forest Grove, Oregon

Student Life (503) 352-2212, Faculty and staff (503) 352-1511, Legal Affairs (503) 352-2236

A University-owned laptop was stolen from a staff member's residence. The stolen laptop was password protected and there is no factual evidence that any private information was stored on the laptop. The computer contained names and some personal information. It does not appear that any Social Security numbers were stored on the system.

Information Source:
Media

records from this breach used in our total: 0

March 19, 2009   **Bailey Middle School**   EDU   PHYS   21
                   Nashville, Tennessee

A Nashville mother who was walking along found confidential paperwork that lists Metro school students' names, Social Security numbers and disabilities. The Metro Schools spokeswoman said they will trace the documents and try to figure out how they got where they weren't supposed to be.

Information Source:
Media

records from this breach used in our total: 21

| March 18, 2009 | **University of West Georgia** **Carrollton, Georgia** | EDU | PORT | 1,300 |

University of West Georgia officials have notified nearly 1,300 students and faculty members that their personal information was on a laptop stolen from a professor traveling in Italy. The laptop was taken last summer, but university officials say they only recently learned that the computer contained sensitive information, including names, addresses, phone numbers and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 1,300

| March 17, 2009 | **Penn State Office of Physical Plant** **University Park, Pennsylvania** | EDU | HACK | 1,000 |

The Social Security numbers of employees working for the Penn State Office of Physical Plant in 2000 may have been stolen. A virus infiltrated an administrative computer that contained more than 1,000 Social Security numbers of OPP employees.

Information Source:
Dataloss DB

records from this breach used in our total: 1,000

| March 16, 2009 | **University of Toledo** **Toledo, Ohio** | EDU | STAT | 24,450 Only 450 were added to the total. |

A computer stolen from the University of Toledo contained personal information for about 24,000 students and 450 faculty during the 2007-08 and 2008-09 academic years. The student data was directory and educational information, such as student identification numbers and grade point averages. The faculty information, however, was more personal and included names, Social Security numbers, birth dates, and more.

Information Source:
Dataloss DB

records from this breach used in our total: 450

| March 11, 2009 | **Binghamton University** **Binghamton, New York** | EDU | STAT | 100,000 |

Binghamton University kept payment information for every student, possibly dating back at least ten years in a storage area next to one of the most trafficked lecture halls on campus, behind a door that was not only unlocked but taped open. The information itself contained Social Security numbers, credit card numbers, scans of tax forms, business information (including Social Security numbers and salary information for employees of students' parents), asylum records and more, all kept in a haphazard and disorganized fashion, sprawled out in boxes, in unlocked (yet lockable) filing cabinets and shelving units. If the information inside the room pertained only to the current students enrolled and their parents that would mean the story would effect, roughly, forty-two thousand people. However, because the information goes back at least ten years, if not more, the potential number of people effect lies well in the hundred thousands.

Information Source:
Media

records from this breach used in our total: 100,000

| March 4, 2009 | **Elk Grove Unified School District** **Elk Grove, California** | EDU | PHYS | 520 |

A document with the Social Security numbers of more than 500 Elk Grove Unified School District employees was lost by a district employee.

Information Source: Dataloss DB

records from this breach used in our total: 520

| March 3, 2009 | **Western Oklahoma State College** **Altus, Oklahoma** | EDU | DISC | 1,500 |

A computer breach at Western Oklahoma State College may have exposed Social Security numbers and other identifying information for 1,500 campus library users. An unauthorized program known as a rootkit was installed on a server administered by an outside party. There is no indication that any of the data on the machine was actually compromised - only that the opportunity for someone to access it existed.

Information Source: Dataloss DB

records from this breach used in our total: 1,500

| February 26, 2009 | **Steamboat Springs School District** **Steamboat Springs, Colorado** | EDU | PORT | 1,300 |

Social Security numbers for 1,300 past and present employees was compromised when a laptop was stolen from the Steamboat Springs School District office. The laptop had a spreadsheet containing the Social Security numbers and names of their owners. The spreadsheet was created as part of a requirement from a past district audit. The laptop was password-protected, but district officials are warning their employees to be on the lookout for any potential identity theft.

Information Source: Dataloss DB

records from this breach used in our total: 1,300

| February 23, 2009 | **University of Florida** **Gainesville, Florida** | EDU | DISC | 101 |

(877) 657-9133 http://privacy.ufl.edu/incidents/2009/ldap

An undated statement on the University's Web site indicates that on January 20, an LDAP Directory Server configuration error allowed outside access to a directory containing Social Secerity numbers and other personal data. Personal data belonging to about 101 people might have been compromised as a result.

Information Source: Dataloss DB

records from this breach used in our total: 101

| February 20, 2009 | **Del Mar College** **Del Mar, California** | EDU | PHYS | 53 |

A class roster containing the names and Social Security numbers of some 53 Del Mar College students has been stolen. The roster was taken out of a professor's vehicle parked at Cole Park. The G.E.D. teacher was taking work home Sunday, when he stopped at Cole Park and his car was broken into.

Information Source: Dataloss DB

records from this breach used in our total: 53

| February 19, 2009 | **University of Florida** **Gainesville, Florida** | EDU | HACK | 97,200 |

(877) 657-9133

A foreign hacker gained access to a University of Florida computer system containing the personal information of students, faculty and staff. The files included the names and Social Security numbers of individuals who used UF's Grove computer system since 1996.

Information Source: Dataloss DB

records from this breach used in our total: 97,200

| February 17, 2009 | **Broome Community College**
Binghamton, New York | EDU | DISC | 14,000 |

Broome Community College, sent out a mailing last week with Social Security number posted prominently on the back cover. The winter/spring 2009 alumni magazine was mailed to 28,000 people, it assumed that less than 14,000 copies had Social Security numbers on the magazine.

Information Source: Dataloss DB

records from this breach used in our total: 14,000

| February 13, 2009 | **University of Alabama**
Tuscaloosa, Alabama | EDU | HACK | 37,000 |

Seventeen of 400 databases were tapped by hackers. Personal information may have been stolen. One of those computers contained lab results for people tested at the campus medical center. The servers had a database containing 37,000 records of lab data. They contain the names, addresses, birthdates and Social Security numbers of each person who has had lab work, such as a blood or urine test, done on the UA campus since 1994.

Information Source: Dataloss DB

records from this breach used in our total: 37,000

| February 6, 2009 | **Purdue University**
West Lafayette, Indiana | EDU | DISC | 962 |

http://news.uns.purdue.edu/Payroll0901.html (http://news.uns.purdue.edu/Payroll0901.html)

A mailing error has resulted in 1099 tax forms being sent to the wrong recipients. The incident affected 248 companies and 962 individuals. Those affected by the incident received letters notifying them that their tax information had either been sent to another or that they themselves had received someone else's information by mistake.

Information Source: Dataloss DB

records from this breach used in our total: 962

| January 31, 2009 | **Ball State University**
Muncie, Indiana | EDU | DISC | 19 |

A employee sent out an e-mail, to verify contact information, to 91 special events staff with an excel spreadsheet attachment that, unbeknownst to the employee, included the Social Security number of 19 of the workers.

Information Source: Dataloss DB

records from this breach used in our total: 19

| January 31, 2009 | **Columbia University**
New York, New York | EDU | PORT | 1,400 |

About 1,400 current, former and prospective students at Columbia University have been told that their personal information, including Social Security numbers, is vulnerable following a security breach. The university said information about the students, as well as some current and

past employees, was on three password-protected notebook computers that were stolen from a Columbia College.

Information Source: Dataloss DB

records from this breach used in our total: 1,400

January 30, 2009	**Kansas State University** **Manhattan, Kansas**	EDU	DISC	45

(785) 532 4441

Students who were enrolled in an agricultural economics class in spring 2001 inadvertently had some personal information exposed on the Internet through a K-State departmental Web site. Names, Social Security numbers and grades of those students have been exposed since 2001.

Information Source: Dataloss DB

records from this breach used in our total: 45

January 21, 2009	**Missouri State University** **Springfield, Missouri**	EDU	DISC	565 Not included in total -- not known how many students have SSNs.

Personal information, including Social Security numbers for 565 foreign students at MSU was leaked this month when a university office sent an e-mail message soliciting their help with language tutoring. The email message they got had a spreadsheet attachment that contained names and Social Security numbers for international students.

Information Source: Dataloss DB

records from this breach used in our total: 0

January 16, 2009	**Southwestern Oregon Community College** **Coos Bay, Oregon**	EDU	PORT	200

A laptop computer was stolen from the campus putting former and current students at risk.

Information Source: Dataloss DB

records from this breach used in our total: 200

January 13, 2009	**University of Oregon** **Eugene, Oregon**	EDU	PORT	Unknown

(541) 346-2510

A laptop computer containing data files for Youth Transition Program (YTP) participants was stolen. Those files contained names and social security numbers.

Information Source: Dataloss DB

records from this breach used in our total: 0

January 12, 2009	**Columbus City Schools** **Columbus, Ohio**	EDU	PHYS	100

Columbus City Schools experienced a security breach, resulting in employees' Social Security numbers being at risk. CPD officers went to

serve drug and auto-theft felony warrants. During the arrest officers learned there might be stolen personal information in the house and found personal information on district employees. It is believed the suspects either stole or intercepted part of a mailing from the payroll division that was en route to annuity companies.

Information Source: Dataloss DB

records from this breach used in our total: 100

| January 11, 2009 | **University of Rochester**
Rochester, New York | EDU | HACK | 450 |

Personal information including Social Security numbers of about 450 current and former University of Rochester students was stolen by hackers this week from a UR database. The information was taken from a non-academic student database and copied illegally to an off-campus IP address.

Information Source: Dataloss DB

records from this breach used in our total: 450

| December 31, 2008 | **Ohio State University**
Columbus, Ohio | EDU | DISC | 18,000 |

http://www.studentlife.osu.edu/dataexposure (http://www.studentlife.osu.edu/dataexposure)

Ohio State University has notified 18,000 current and former students that their personel information was mistakenly stored on a computer server exposed to the Internet. The data included student names, Social Security numbers, addresses and coverage dates for those enrolled in the health insurance plan for three quarters in 2005-06.

Information Source: Dataloss DB

records from this breach used in our total: 18,000

| December 23, 2008 | **Ohio University-Chillicothe**
Chillicothe, Ohio | EDU | PORT | 38 |

An external computer hard drive was discovered missing or stolen. Current and former wellness center members' Social Security numbers were on the hard drive.

Information Source: Dataloss DB

records from this breach used in our total: 38

| December 22, 2008 | **University of North Carolina School of the Arts**
Winston-Salem, North Carolina | EDU | DISC | 2,700 |

Names and Social Security numbers may have been accidentally exposed in a security breach involving a university computer server. The security breach occurred in May of 2006 and affected students who were enrolled between 2003 and 2006.

Information Source: Dataloss DB

records from this breach used in our total: 2,700

| December 19, 2008 | **Austin Peay State University**
Clarksville, Tennessee | EDU | PHYS | 750 |

Two computers containing personal information were stolen. The computers contained names and Social Security numbers of students.

Information Source: Dataloss DB

records from this breach used in our total: 750

| December 15, 2008 | **University of North Carolina** **Greensboro, North Carolina** | EDU | HACK | Unknown |

A breach of the accounting computer systems at UNC-Greensboro may have exposed personal employee information to intruders. The breach was detected on a computer in the Accounting Services office, in the form of a virus that may have allowed unauthorized access.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| December 12, 2008 | **Oregon Health & Science University** **Portland, Oregon** | EDU | PORT | 890 |

A laptop stolen in Chicago this week contained health records. It was stolen from a hotel while an OHSU employee was there on business. The data could include medical record numbers, names, telephone numbers, dates of birth, gender, Social Security numbers, addresses.medical diagnosis category and category of treatment - but not the specific treatments.

Information Source:
Dataloss DB

records from this breach used in our total: 890

| December 5, 2008 | **Cal Poly Pomona** **Pomona, California** | EDU | DISC | 675 |

A student informed the university that he accessed an Excel file containing his personal information and others while on the Internet. The information includes names, addresses, phone numbers and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 675

| November 21, 2008 | **Jackson-Madison County School System** **Jackson, Tennessee** | EDU | PORT | 200 |

A computer disk containing Social Security numbers and test scores was stolen from a principal's car.

Information Source:
Dataloss DB

records from this breach used in our total: 200

| November 12, 2008 | **University of Florida College of Dentistry** **Gainesville, Florida** | EDU | HACK | 330,000 |

Some current and former dental patients have been notified that an unauthorized intruder recently accessed a College of Dentistry computer server storing their personal information. College information technology staff members were upgrading the server and found software had been installed on it remotely. Information stored on the server included names, addresses, birth dates, Social Security numbers and, in some cases, dental procedure information for patients dating back to 1990.

Information Source:
Dataloss DB

records from this breach used in our total: 330,000

| November 11, 2008 | **Sinclair Community College** **Dayton, Ohio** | EDU | DISC | 1,000 |

The names and Social Security numbers of almost 1,000 employees were inadvertently left open to public view on the Internet for about a year. A spreadsheet with information on people who worked at the school in 2000 and 2001 was placed in a computer folder by an employee. The employee didn't realize the folder could be viewed on the Internet.

Information

Source: Dataloss DB				*records from this breach used in our total: 1,000*

November 9, 2008	**Texas A&M University Corpus Christi, Texas**	EDU	DISC	1,430

Through an Internet search on the university's Web site, a student viewed a document that listed admissions applicants from 2005. The page listed names and Social Security numbers.

Information Source: Dataloss DB				*records from this breach used in our total: 1,430*

November 6, 2008	**Harvard Law School Cambridge, Massachusetts**	EDU	PORT	21,000

A computer tape containing Social Security numbers, addresses, and financial information was either lost or stolen. About 8,000 records of present and former clients contained Social Security numbers another 13,000 had other identification information that was contained on the tape.

Information Source: Dataloss DB				*records from this breach used in our total: 21,000*

November 3, 2008	**Genesee Intermediate School District Mundy Township, Michigan**	EDU	PORT	6,000 Not included in total.

A laptop stolen had been used for background checks on school workers and included their fingerprints and some personal information such as their names, addresses, birthdates and race. The laptop did not have Social Security numbers and the data was stored in files that require a password to be opened.

Information Source: Media				*records from this breach used in our total: 0*

November 1, 2008	**Seattle School District Seattle, Washington**	EDU	DISC	5,000

Personal information, including Social Security numbers, was inadvertently released to a local union representing some district workers. The 5,000 employees are more than half the district's work force. Included were about 700 members of International Union of Operating Engineers Local 609, which represents custodial, nutritional services, security- and alarm-monitoring workers.

Information Source: Dataloss DB				*records from this breach used in our total: 5,000*

October 24, 2008	**Shenendehowa Transportation Employees Shenendehowa, New York**	EDU	HACK	250

A Shenendehowa sophomore was arrested after he allegedly accessed the personal data of some 250 transportation employees due to a school district error in configuring information on a new computer server. The student was able to use his student password to access an employee domain and 250 names of past and present Shenendehowa transportation employees, their Social Security numbers, driver's license numbers and more.

Information Source: Dataloss DB				*records from this breach used in our total: 250*

| October 13, 2008 | **Southwest Mississippi Community College** **Summitt, Mississippi** | EDU | DISC | 1,000 |

Former Southwest Mississippi Community College students had some of their personal information made available temporarily on the Internet. The breach involved names, addresses, and in some cases, Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 1,000

| October 7, 2008 | **University of North Dakota Alumni Association** **Grand Forks, North Dakota** | EDU | PORT | 84,554 |

A laptop computer containing sensitive personal and financial information on alumni, donors and others was stolen from a vehicle belonging to a software vendor retained by the UND. The information, included individuals' credit card and Social Security numbers,

Information Source:
Dataloss DB

records from this breach used in our total: 84,554

| September 30, 2008 | **University of Indianapolis** **Indianapolis, Indiana** | EDU | HACK | 11,000 |

A hacker attacked the University of Indianapolis' computer system and gained access to personal information and Social Security numbers for 11,000 students, faculty and staff,

Information Source:
Dataloss DB

records from this breach used in our total: 11,000

| September 26, 2008 | **Fort Wayne Community Schools** **Fort Wayne, Indiana** | EDU | UNKN | 3,348 |

A man arrested on forgery and counterfeiting charges may have used some employees' personal information in his possession. A 94-page document containing personal information belonging to 3,348 FWCS employees was found by police. The information included names, Social Security numbers, dates of birth and salary.

Information Source:
Dataloss DB

records from this breach used in our total: 3,348

| September 22, 2008 | **Sonoma State University** **Sonoma, California** | EDU | DISC | 600 |

Social Security numbers have been exposed to the public through an internal department website.

Information Source:
Dataloss DB

records from this breach used in our total: 600

| September 19, 2008 | **Texas A&M University** **College Station, Texas** | EDU | HACK | 31 |

A class roster was among some documents located on a computer server that was hacked. The class roster was for Economics-2301 held during the first summer session of 2004. Social Security numbers were part of the information on those documents.

Information Source:
Dataloss DB

records from this breach used in our total: 31

| September 12, 2008 | **Tennessee State University** **Nashville, Tennessee** | EDU | PORT | 9,000 |

A flash drive containing the financial information and Social Security numbers of students was reported missing. The flash, which contained financial records of TSU students dating back to 2002.

Information Source: Dataloss DB

records from this breach used in our total: 9,000

| September 11, 2008 | **Marshall University** **Charleston, West Virginia** | EDU | DISC | 198 |

The names and Social Security numbers of Marshall University students were openly available on the Internet.

Information Source: Dataloss DB

records from this breach used in our total: 198

| September 11, 2008 | **University of Iowa College of Engineering** **Iowa City, Iowa** | EDU | HACK | 500 |

Some students are being notified by the College that their personal information may have been exposed in a recent computer breach. The compromised computer contained a file with names and Social Security numbers of students stored on its hard drive.

Information Source: Dataloss DB

records from this breach used in our total: 500

| September 10, 2008 | **Ivy Tech Community College** **Bloomington, Indiana** | EDU | DISC | Unknown |

http://www.ivytech.edu/about/security/ (http://www.ivytech.edu/about/security/)

An employee of the college used an internal file sharing system to send a file that consisted of students enrolled in the spring 2008 semester for distance education courses. The employee intended to share the file with a single employee of the college. Instead, due to a clerical error, the invitation to view the file was sent to a list of all Indianapolis region employees.

Information Source: Dataloss DB

records from this breach used in our total: 0

| September 9, 2008 | **University of Pittsburgh** **Pittsburgh, Pennsylvania** | EDU | PORT | Unknown |

A laptop containing personal information including names and Social Security numbers was stolen. The laptop, stolen from Mervis Hall was being used by an employee to conduct surveys of alumni that are used in college rankings.

Information Source: Dataloss DB

records from this breach used in our total: 0

| September 5, 2008 | **East Burke High School** **Morganton, North Carolina** | EDU | DISC | 163 |

For the past five years, East Burke High School's web site exposed files containing personal information including names, Social Security numbers, addresses, phone numbers, job titles, email addresses and unlisted phone numbers of teachers, bus drivers, custodians and other staff members on the Internet.

Information

Source:
Dataloss DB

records from this breach used in our total: 163

September 2,
2008

**Clarkson University
Potsdam, New York**

EDU   DISC   245

A non-malicious student intruder gained access to a restricted server and promptly reported the vulnerability to campus authorities. Approximately 245 employees and former employees had personal information, including name, social security number, and date of birth, compromised during the security breach. The file containing personal information was a record of employees that had university credit cards known as purchase cards (or p-cards). Any university member requesting a p-card must provide their Social Security number and date of birth on the application form.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 245

August 30, 2008

**National Technical Institute for the Deaf and Rochester Institute of Technology
Rochester, New York**

EDU   PORT   13,800

RIT Hotline through 9/26/08 (866) 624-8330, RIT Public Safety (585) 475-2853

http://www.rit.edu/news/?v=46283 (http://www.rit.edu/news/?v=46283)

A recently stolen laptop contained the names, birth dates and Social Security numbers of about 12,700 applicants to the National Technical Institute for the Deaf and another 1,100 people at Rochester Institute of Technology. The laptop belonged to an employee and was stolen on Monday from an office at NTID. People at RIT, who are not affiliated with NTID, are affected because their personal information was being used as part of a control group in an internal study.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 13,800

August 28, 2008

**Reynoldsburg Ohio City School District
Reynoldsburg, Ohio**

EDU   PORT   4,259

Reynoldsburg school officials were phasing out the use of Social Security numbers in the district's student database when someone stole a laptop containing that information. The district laptop, taken from a computer technician's car, also included names, addresses and phone numbers for two-thirds of the district's enrollment.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 4,259

August 27, 2008

**Kansas State University
Manhattan, Kansas**

EDU   PHYS   86

An instructor for classes offered through the Division of Continuing Education, taught through the UFM Community Learning Center, reported an overnight theft of numerous items from a car, which was parked outside a Manhattan residence. Items taken included a backpack with a list of names and Social Security numbers of 86 K-State students who had taken that instructor's classes from fall 2007 through summer 2008.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 86

August 26, 2008

**Prince William County Public Schools
Manassas, Virginia**

EDU   DISC   2,600

Personal information of some students, employees and volunteers was accidentally posted online by a Prince William County Public Schools employee. Information for more than 2,600 people was exposed through a file-sharing program by an employee working from

home on a personal computer. The compromised information included: names, addresses and student identification numbers of more than 1,600 students names and Social Security numbers of 65 employees other confidential information for about 250 employees and the names, addresses and e-mail addresses of more than 700 volunteers.

Information Source:
Dataloss DB

records from this breach used in our total: 2,600

| August 18, 2008 | **Keller High School**
Keller, Texas | EDU | DISC | 45 |

Keller family's received a mailing from Keller High School last week. Upon opening it, they found two enrollment forms. One was an emergency-care authorization form. But the other was a student information form containing another classmate's Social Security number, student ID number, home address, phone number and contact information for his parents at home and at work. They quickly realized that their child's private information, which they used to set up their college fund and other accounts, was mailed to someone else.

Information Source:
Dataloss DB

records from this breach used in our total: 45

| August 18, 2008 | **The Princeton Review**
New York, New York | EDU | DISC | 108,000 (No SSNs or financial information reported) |

The test-preparatory firm accidentally published the personal data and standardized test scores of tens of thousands of Florida students on its Web site. One file on the site contained information on about 34,000 students in the public schools in Sarasota, Fl. Another folder contained dozens of files with names and birth dates for 74,000 students in the school system of Fairfax County, Va.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| August 4, 2008 | **Arapahoe Community College**
Littleton, Colorado | EDU | PORT | 15,000 |

A contractor who manages the student information database had a flash drive lost or stolen. Information on the drive included the names, addresses, credit card numbers and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 15,000

| August 3, 2008 | **Oakland School District**
Oakland, California | EDU | STAT | Unknown |

Thieves stole 10 desktop computers containing employees' personal information from the Oakland school district's main office. District officials are still determining what information was on each computer, but the machines may contain personal information provided to the district when employees were hired. It is unknown how many employees' records were on the computers.

Information Source:
Media

records from this breach used in our total: 0

| July 31, 2008 | **University of Texas, Dallas**
Dallas, Texas | EDU | HACK | 9,100 |

http://www.utdallas.edu/infosecurity/ (http://www.utdallas.edu/infosecurity/)

A security breach in UTD's computer network may have exposed Social Security numbers along with names, addresses, email addresses or telephone numbers: *4,406* students who were on the Dean's List or graduated between 2000 and 2003; *3,892* students who were contacted to take part in a survey by the Office of Undergraduate Education in 2002; *88* staff members from Facilities Management; *716* faculty and staff members listed in a space inventory record from 2001.

Information Source:
Dataloss DB

records from this breach used in our total: 9,100

| July 26, 2008 | **Connecticut College, Wesleyan University, Trinity College** **Middletown, Connecticut** | EDU | HACK | 2,815 |

A Connecticut College library system was breached by hackers apparently looking to set up chat rooms or send spam e-mails. The system's database included the names, addresses and Social Security or driver's license numbers of approximately 2,800 Connecticut College library patrons, 12 Wesleyan University patrons and three from Trinity.

Information Source:
Dataloss DB

records from this breach used in our total: 2,815

| July 25, 2008 | **Ohio University College of Osteopathic Medicine** **Columbus, Ohio** | EDU | DISC | 492 |

http://www.ohiocore.org/answers (http://www.ohiocore.org/answers) , (866) 437-8698

A clerical error led to the online posting of the names and Social Security numbers of people who spoke at Ohio University's Centers for Osteopathic Research and Education. A spreadsheet that contained the information had been accessible since March 20 and was discovered when a nurse found the information last week while conducting online research. In addition to names and Social Security numbers, the spreadsheet included contact numbers, addresses, their speaking topics and federal employer identification numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 492

| July 24, 2008 | **Hillsborough Community College** **Tampa, Florida** | EDU | PHYS | 2,000 |

Hillsborough Community College warned its employees to monitor their bank accounts because an HCC programmer's laptop was stolen from a hotel parking lot in Georgia. The programmer had been working on a payroll project for a group of employees using their names, bank-routing numbers, retirement information and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 2,000

| July 24, 2008 | **University of Houston** **Houston, Texas** | EDU | DISC | 259 |

The names and Social Security numbers of University of Houston students were inadvertently posted on the Internet for more than two years. The posting occurred when a math department lecturer posted student grades on a UH Web server in October 2005.

Information Source:
Dataloss DB

records from this breach used in our total: 259

| July 17, 2008 | **University of Maryland** **College Park, Maryland** | EDU | DISC | 23,000 |

University of Maryland accidentally released the addresses and Social Security numbers of thousands of students. A brochure with on-

campus parking information was sent by U.S. Mail to students. The University discovered the labels on the mailing had the students' Social Security numbers on it.

Information Source:
Dataloss DB   *records from this breach used in our total: 23,000*

| July 16, 2008 | **Indiana State University**
Terre Haute, Indiana | EDU | PORT | 2,500 |

A password-protected laptop computer containing personal information for current and former Indiana State University students was stolen. The laptop contained data for students who took economics classes from 1997 through the spring semester 2008. The information includes names, grades, e-mail addresses and student identification numbers and in some cases Social Security numbers.

UPDATE(7/22/08) :The laptop computer was mailed anonymously back to the professor it was stolen from six days after it was stolen along with other personal items.

Information Source:
Dataloss DB   *records from this breach used in our total: 2,500*

| July 15, 2008 | **University of Texas, Austin**
Austin, Texas | EDU | DISC | 2,500 |

The personal information of University of Texas students and faculty has been exposed on the Internet. An independent watchdog discovered more than five dozen files containing confidential graduate applications, test scores, and Social Security numbers. The files were inadvertently posted by at least four different UT professors to a file server for the School of Biological Sciences.

Information Source:
Dataloss DB   *records from this breach used in our total: 2,500*

| July 10, 2008 | **Williamson County (TN) Schools**
Franklin, Tennessee | EDU | DISC | 5,100 |

Social Security numbers and other personal information of 4,000 children were posted on the Internet.

UPDATE 7/11/08 : 5, 100 students' information may be compromised.

Information Source:
Dataloss DB   *records from this breach used in our total: 5,100*

| July 2, 2008 | **University of Nebraska, Kearney**
Kearney, Nebraska | EDU | HACK | 2,035 |

(308) 865-8950

Officials at the University of Nebraska at Kearney discovered a security breach involving nine university computers. Of the nine computers involved, five contained names and partial or complete Social Security numbers.

Information Source:
Dataloss DB   *records from this breach used in our total: 2,035*

| June 24, 2008 | **Southeast Missouri State University**
Cape Girardeau, Missouri | EDU | INSD | 800 |

(573) 986-6800, (573) 335-6611, ex.123,lbavolek@semissourian.com

A former employee has been indicted on two charges of identity fraud and one charge of computer trespass after being found in possession of 800 student names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 800

| June 12, 2008 | **Columbia University**
New York, New York | EDU | DISC | 5,000 |

Social Security numbers of some 5,000 Columbians were accidentally posted by a student employee on a Google-hosted site in February 2007. Student Services discovered the leak in June 2008 and removed the sensitive data after it had been available for 16 months.

Information Source:
Dataloss DB

records from this breach used in our total: 5,000

| June 11, 2008 | **Dickson County Board of Education**
Dickson, Tennessee | EDU | PORT | 850 |

A computer containing sensitive personal information was stolen from the Dickson County Board of Education. The computer belongs to the new director of schools and was loaded with the name and Social Security number of every school employee from the 2006-2007 school year, a total of 850.

Information Source:
Dataloss DB

records from this breach used in our total: 850

| June 10, 2008 | **University of Florida**
Gainesville, Florida | EDU | DISC | 11,300 |

Current and former students had their Social Security numbers, names and addresses accidentally posted online. The information became available when former student employees of the Office for Academic Support and Institutional Service, or OASIS, program created online records of students participating in the program between 2003 and 2005.

Information Source:
Dataloss DB

records from this breach used in our total: 11,300

| June 9, 2008 | **University of South Carolina**
Columbia, South Carolina | EDU | STAT | 7,000 |

Several items were stolen from an office in the Moore School of Business. Among the items was a desktop computer. As a result of the computer being stolen, it is possible that some personally identifiable data could have been compromised.

Information Source:
Dataloss DB

records from this breach used in our total: 7,000

| June 7, 2008 | **East Tennessee State University**
Johnson City, Tennessee | EDU | STAT | 6,200 |

6,200 people may have had there identities compromised by the theft of a desktop computer. The computer is password protected and files cannot be easily accessed. But there is a small possibility that the information could be compromised.

Information Source:
Dataloss DB

records from this breach used in our total: 6,200

June 6, 2008	**Stanford University** **Stanford, California**	EDU	PORT	72,000

Stanford University determined that a university laptop, which was recently stolen, contained confidential personnel data. The university is not disclosing details about the theft as an investigation is under way.

Information Source:
Dataloss DB

records from this breach used in our total: 72,000

June 4, 2008	**Oregon State University** **Corvallis, Oregon**	EDU	HACK	4,700

The Oregon State Police are investigating the theft of personal information from online customers of the OSU Bookstore who used credit cards to purchase items.

Information Source:
Dataloss DB

records from this breach used in our total: 4,700

May 31, 2008	**Pocono Mountain School District** **Swiftwater, Pennsylvania**	EDU	HACK	11,000

 (570) 873-7121, ext. 10151

A hacker apparently broke into the computers at Pocono Mountain School District and may have tapped into confidential information concerning students and their parents. Information may have included the students' birth dates, Social Security numbers, student IDs, home phones, and the parents' names, phone numbers and emergency phone numbers. "If you see any unauthorized activity, promptly contract your service provider and or the office of the director of technology at 570-873-7121, ext. 10151."

Information Source:
Dataloss DB

records from this breach used in our total: 11,000

May 28, 2008	**University of California, San Francisco** **San Francisco, California**	EDU	HACK	3,569

(415) 353-7427, [PathHotline@ucsf.edu (mailto:PathHotline@ucsf.edu)](mailto:PathHotline@ucsf.edu)

During routine monitoring of a campus computer network, UCSF discovered unusual data traffic on one of its computers. During the investigation, UCSF determined that an unauthorized movie-sharing program had been installed on one computer by an unknown individual. Installation of this program required high-level system access. The computer contained files with lists of patients from the UCSF pathology department's database. The data included information such as patient names, dates of pathology service, health information and, in some cases, Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 3,569

May 20, 2008	**New York University** **New York, New York**	EDU	DISC	273

Duke University's Fuqua School of Business is notifying former New York University students that some of their personal information was inadvertently accessible by targeted Internet searches. The personal data included names and Social Security numbers and was contained in the faculty member's research records. The information could have been accessed only if searched by specific student names, along with a search code for Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 273

| May 17, 2008 | **University of Louisville**
Louisville, Kentucky | EDU | PHYS | 20 |

Documents being copied and taken from a private office in the president's office, to its Internal Audit Office and Department of Public Safety may have resulted in a security breach. The documents contained personal information - including Social Security numbers, student and employee identification numbers and salary information - for current and recent student employees. The university learned of the theft when salary information was shared anonymously with some employees in the office.

Information Source:
Dataloss DB

records from this breach used in our total: 20

| May 16, 2008 | **Spring Independent School District (Spring, TX)**
Spring, Texas | EDU | PORT | 8,000 |

A laptop computer containing the personal information of students was stolen from a employee's car. The car burglars made off with her school laptop and an external flash drive. The flash drive contains students' Social Security numbers, personal information, schools those students attend, as well as their grade level and birthdates. The drive also contained the Texas Assessment of Knowledge and Skills test results.

Information Source:
Dataloss DB

records from this breach used in our total: 8,000

| May 16, 2008 | **Greil Memorial Psychiatric Hospital**
Montgomery, Alabama | EDU | PHYS | Unknown |

Index cards containing patients personal information, names, dates of birth, even Social Security numbers are gone. Hundreds of records have simply disappeared.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 16, 2008 | **Chester County School District**
Downingtown, Pennsylvania | EDU | HACK | 55,000 |

A 15-year-old student gained access to files on a computer at Downingtown West High School. Private information, including names, addresses and Social Security numbers, of more than 50,000 people were accessed. The student apparently used a flash drive to save the personal data of about 40,000 taxpayers and 15,000 students.

Information Source:
Media

records from this breach used in our total: 55,000

| May 14, 2008 | **Oklahoma State University**
Stillwater, Oklahoma | EDU | HACK | 70,000 |

A breach in an Oklahoma State University computer server exposed names, addresses and Social Security numbers of students, staff and faculty who bought parking and transit services permits in the past six years.

Information Source:
Dataloss DB

records from this breach used in our total: 70,000

| May 9, 2008 | **Princeton University Tower Club**
Princeton, New Jersey | EDU | DISC | 103 |

Tower Club is taking steps to protect 103 of its alumni in the classes of 2006 and 2007 after a spreadsheet listing their names and Social

Security numbers was e-mailed to current club members. The document was attached to an apparently unrelated e-mail that informed current members about a club event. The spreadsheet was attached unintentionally because of a technical glitch in an email program.

Information Source:
Dataloss DB

records from this breach used in our total: 103

| May 8, 2008 | **Dominican University**
River Forest, Illinois | EDU | HACK | 5,000 |

Two students were able to access records on a staff network storage area. The files accessed were three spreadsheets that included students' names, addresses, phone numbers, birthdays and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 5,000

| May 8, 2008 | **Las Cruces Public Schools**
Las Cruces, New Mexico | EDU | DISC | 1,800 |

A part-time computer analyst for Las Cruces Public Schools inadvertently posted personal data for 50 special education students and 1,750 district employees on the Internet. Information posted included Social Security number, date of birth, name, the nature of disability and caseworker's name.

Information Source:
Dataloss DB

records from this breach used in our total: 1,800

| May 6, 2008 | **Ohio State University Agricultural Technical Institute**
Wooster, Ohio | EDU | DISC | 192 |

Personal information on faculty and staff members was accidentally emailed to about 680 students. The email contained spreadsheet information listing the names, positions, salaries and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 192

| April 25, 2008 | **University of Colorado, Boulder**
Boulder, Colorado | EDU | HACK | 9,500 revised to 0 |

Three computers in the Division of Continuing Education and Professional Studies were compromised, leaving people open to potential identity theft. One of the three computers had personal data, including names, Social Security numbers, addresses and grades.

UPDATE (5/1/08): Upon further analysis, the University concluded that no personal data had been exposed. 9,500 records were initially thought to be comprised, but later this was revised to zero.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 23, 2008 | **Southern Connecticut State University**
New Haven, Connecticut | EDU | HACK | 11,000 |

Southern Connecticut State University is taking action to prevent its students from becoming victims of identity theft. The move comes after a website with student and alumni information was found to be easily accessible to hackers. It appears that no financial information was accessed but Social Security numbers were vulnerable.

Information Source:

records from this breach used in our total: 11,000

Dataloss DB

| April 16, 2008 | **Hexter Elementary School**
Dallas, Texas | EDU | PHYS | Unknown |

Employee and volunteer records were found at a recycling bin near the school. It's unknow what type of documents were found.

Information Source:
Media

records from this breach used in our total: 0

| April 16, 2008 | **University of Virginia**
Charlottesville, Virginia | EDU | PORT | 7,000 |

A laptop stolen from a University of Virginia employee contained sensitive information about students, staff and faculty members. Stolen from an unidentified employee from an undisclosed location in Albemarle County, the laptop contained a confidential file filled with names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 7,000

| April 14, 2008 | **Stokes County High Schools**
Danbury, North Carolina | EDU | STAT | 800 |

A school computer containing the names, test scores and Social Security numbers of students from three Stokes County high schools was stolen from a locked closet.

Information Source:
Dataloss DB

records from this breach used in our total: 800

| April 13, 2008 | **University of Toledo**
Toledo, Ohio | EDU | DISC | 6,488 |

Personal information of the University of Toledo employees, the majority having worked on the Health Science Campus in 1993 and 1999 - last month was inadvertently placed on a server to which all employees had access. The information, which was used for payroll purposes, included names, addresses, and Social Security numbers and was accessible for about 24 hours.

Information Source:
Dataloss DB

records from this breach used in our total: 6,488

| April 12, 2008 | **West Seneca School District**
West Seneca, New York | EDU | HACK | 1,800 |

Several current and former students are believed to have broken into the school district's computer system and copied secure files that included the personal information and Social Security numbers of school employees

Information Source:
Dataloss DB

records from this breach used in our total: 1,800

| April 10, 2008 | **Joliet West High School**
Joliet, Illinois | EDU | HACK | Unknown |

A student using a school computer last month was able to access personal information about every student enrolled. The student allegedly downloaded a list of names and Social Security numbers to his iPod.

Information

Source:
Dataloss DB

records from this breach used in our total: 0

| April 4, 2008 | **University of California, Irvine**
Irvine, California | EDU | UNKN | 7,000 |

7,000 current or former graduate students could be at risk of identity thieves who already used stolen data to file fake tax returns for 93 students. UCI does not know how the information was stolen or who is using it.

UPDATE (10/22/10): A class action lawsuit against United Healthcare Services was settled. UCI graduate students were affected by a fraudulent tax return scheme after an employee of United Healthcare Services misused their information to file fraudulent tax returns.

Information Source:
Dataloss DB

records from this breach used in our total: 7,000

| March 28, 2008 | **Antioch University**
Yellow Springs, Ohio | EDU | HACK | 70,000 |

A computer system that contained personal information on about 70,000 people was breached by an unauthorized intruder three times. The system contained the names, Social Security numbers, academic records and payroll documents for current and former students, applicants and employees.

Information Source:
Dataloss DB

records from this breach used in our total: 70,000

| March 26, 2008 | **Broward School District**
Coconut Creek, Florida | EDU | HACK | 38,000 |

An Atlantic Technical High School senior hacked into a district computer and collected Social Security numbers and addresses of district employees.

Information Source:
Dataloss DB

records from this breach used in our total: 38,000

| March 22, 2008 | **Western Carolina University**
Cullowhee, North Carolina | EDU | HACK | 555 |

Someone had hacked into a computer server and had access to the Social Security numbers of 555 graduates of the university who had signed up for a newsletter.

Information Source:
Dataloss DB

records from this breach used in our total: 555

| March 20, 2008 | **Lasell College**
Newton, Massachusetts | EDU | HACK | 20,000 |

A hacker accessed data containing personal information on current and former students, faculty, staff and alumni. Information included names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 20,000

| March 17, 2008 | **Binghamton University**
Binghamton, New York | EDU | DISC | 300 |

A university employee mistakenly sent an e-mail attachment containing the names, grade point averages and Social Security numbers of junior and senior accounting students to another group of School of Management students.

Information Source:
Dataloss DB

records from this breach used in our total: 300

| March 12, 2008 | **Harvard University**
Cambridge, Massachusetts | EDU | HACK | 6,600 |

Harvard Graduate School of Arts and Sciences (GSAS) Web server may have compromised 10,000 sets of personal information from applicants and students, including 6,600 Social Security numbers and 500 Harvard ID numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 6,600

| February 16, 2008 | **Texas A&M University**
College Station, Texas | EDU | DISC | 3,000 |

A computer file containing the names and Social Security numbers of current and former Texas A&M University agricultural employees was inadvertently posted online and accessible to the public for three weeks.

Information Source:
Dataloss DB

records from this breach used in our total: 3,000

| February 13, 2008 | **Middle Tennessee State University**
Murfreesboro, Tennessee | EDU | STAT | 1,500 |

A professor left the university computer unattended in the mass communication department about two weeks ago and an unidentified person is believed to have used the machine to send spam e-mails. The computer contained the names and Social Security numbers of past and current students.

Information Source:
Dataloss DB

records from this breach used in our total: 1,500

| February 12, 2008 | **Long Island University**
Brookville, New York | EDU | PHYS | 30,000 |

Students tax forms mailed to them last week in were in defective mailers. The mailers containing each student's annual 1098-T Tuition Statement were supposed to have adhesive on all four sides. But one side of each envelope was missing adhesive. The statement contains the student's name, address and Social Security number.

Information Source:
Dataloss DB

records from this breach used in our total: 30,000

| February 12, 2008 | **Modesto City Schools**
Modesto, California | EDU | PORT | 3,500 |

 (209) 576-4192

A computer hard drive holding the names, addresses, birth dates and Social Security numbers of Modesto City Schools' employees was stolen.

UPDATE (2/15/08): The breach has been attributed to a computer theft that affected a contractor named Systematic Automation Inc. Nineteen organizations were affected by the incident.

Information
Source:
Dataloss DB

records from this breach used in our total: 3,500

| February 11, 2008 | **Jefferson County Public Schools**
Arvada, Colorado | EDU | PORT | 2,900 |

A special education technician had a personal laptop and jump drive stolen during a home robbery. Student name and date of birth, Student ID number, School location If the student has received district transportation additional information such as parent or guardian name and contact information, may also have been on the jump drive. The stolen information did not contain any Social Security numbers or financial information.

Information
Source:
Dataloss DB

records from this breach used in our total: 2,900

| January 30, 2008 | **University of Massachusetts Dartmouth**
Dartmouth, Massachusetts | EDU | DISC | 32 (No full SSNs reported) |

A privacy organization discovered the names, grades, GPAs and partial Social Security numbers of 32 former students. It appears that the information is from a Fall of 2004 CIS 100 class. The discovery was made in December and all affected students were informed by March 3 of 2008.

Information
Source:
Dataloss DB

records from this breach used in our total: 0

| January 29, 2008 | **Georgetown University**
Washington, District Of Columbia | EDU | PORT | 38,000 |

A hard drive containing the Social Security numbers of Georgetown students, alumni, faculty and staff was reported stolen from the office of Student Affairs.

Information
Source:
Dataloss DB

records from this breach used in our total: 38,000

| January 25, 2008 | **Penn State University**
University Park, Pennsylvania | EDU | PORT | 677 |

A university laptop containing archived information and Social Security numbers for 677 students attending Penn State between 1999 and 2004 was recently stolen from a faculty member.

Information
Source:
Dataloss DB

records from this breach used in our total: 677

| January 25, 2008 | **Murray State University**
Murray, Kentucky | EDU | DISC | 260 |

The personal information of students and professionals who attended Murray State was found online. Names, Social Security numbers, dates of birth and other personal information had been posted in a publicly accessible report titled "2000-2001 State Admissions Report." It seems someone manipulated the Excel file to reveal confidential information. The report should have been posted as a PDF. The information was pulled from the website and affected individuals were contacted shortly after Murray was notified of the breach.

Information

Source:
Dataloss DB

records from this breach used in our total: 260

January 23, 2008 | **Baylor University** | EDU | INSD | Unknown
Waco, Texas

A student employee breached the security of the Baylor Information Network to access the Bear ID and passwords of those logging on to the BIN. This access didn't include sensitive information like Social Security Numbers, financial information or academic records. It was just unlawful access to Bear IDs and passwords. The information did, however, give access to Baylor e-mail and Blackboard accounts.

*Information
Source*:
Media

records from this breach used in our total: 0

January 18, 2008 | **Colorado State University** | EDU | DISC | 300
Fort Collins, Colorado

A privacy group discovered four files containing sensitive personal student information online. Students with some connection to the Warner College of Natural Resources had their Social Security numbers, usernames, passwords and other information posted sometime between 2000 and 2004. The breach was discovered on November 15 of 2007.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 300

January 16, 2008 | **University of Wisconsin, Madison** | EDU | DISC | 205
Madison, Wisconsin

The personal information, including e-mail addresses, phone numbers, Social Security numbers and campus ID numbers of faculty and staff who made purchases from the DoIT computer shop had been accessible on a campus Internet site.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 205

January 14, 2008 | **Tennessee Tech University** | EDU | PORT | 990
Cookeville, Tennessee

A portable storage drive containing the names and Social Security numbers of 990 students has been lost. A school employee transferred the information onto a portable flash drive when the printer where he was working did not print. The employee noticed the drive was missing the next morning.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 990

January 12, 2008 | **California State University Stanislaus, Sodexho** | EDU | UNKN | Unknown
Turlock, California

A possible data breach occurred on a food vendor's computer server. Credit card numbers, cardholder names and expiration dates were exposed, leaving hundreds, possibly thousands, of university students, staff and guests open to identity theft, with victims reporting fake charges on their cards. Social Security numbers were not accessible.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 0

January 11, 2008 | **University of Akron** | EDU | PORT | 800
Akron, Ohio

A portable hard drive containing personal information is missing and may have been discarded or destroyed. The device contained Social Security numbers, names and addresses of students and graduates.

Information Source:
Dataloss DB

records from this breach used in our total: 800

| January 11, 2008 | **University of Iowa**
Iowa City, Iowa | EDU | DISC | 216 |

Iowa College of Engineering has notified some of its former students that some of their personal information, including Social Security numbers, was inadvertently exposed on the Internet for several months.

Information Source:
Dataloss DB

records from this breach used in our total: 216

| January 8, 2008 | **University of Georgia**
Athens, Georgia | EDU | HACK | 4,250 |

Former and prospective residents of a University housing complex were affected by a hacker who was able to access a server containing personal information, including Social Security numbers. A computer with an overseas IP address was able to access the personal information - including Social Security numbers, names and addresses - of 540 current graduate students living in graduate family housing and 3,710 former students and applicants.

Information Source:
Dataloss DB

records from this breach used in our total: 4,250

| January 7, 2008 | **Franklin University**
Columbus, Ohio | EDU | DISC | 6,440 |

A file with student and alumni information was accidentally placed on a publicly accessible web server. The information included names, Social Security numbers, term and class information, email addresses and Franklin University ID numbers. The file was removed from the web server.

Information Source:
Dataloss DB

records from this breach used in our total: 6,440

| January 7, 2008 | **Central Piedmont Community College**
Charlotte, North Carolina | EDU | INSD | 3,437 |

An employee reported unauthorized credit card charges. An investigation revealed that a part-time employee had used the employee's password and accessed personal information.

Information Source:
Dataloss DB

records from this breach used in our total: 3,437

| January 5, 2008 | **New Mexico State University**
Las Cruces, New Mexico | EDU | PORT | Unknown |

A computer hard drive containing the names and Social Security numbers of current and former NMSU employees is missing from the Pan American Center.

Information Source:

records from this breach used in our total: 0

Dataloss DB

| January 5, 2008 | **University of Texas Austin**
Austin, Texas | EDU | DISC | 13 |

A privacy group discovered a file with the names, Social Security numbers, test scores, assignment scores and grades of 13 people online. It appears that the file was accidentally placed there by a professor who taught Biology 331. The discovery was made on November 3 of 2007 and the University took the file offline within hours of notification.

Information Source:
Dataloss DB

records from this breach used in our total: 13

| January 3, 2008 | **Dorothy Hains Elementary School**
Augusta, Georgia | EDU | STAT | Unknown |

The library door was kicked in and the circulation computer was stolen, something the principal desperately wants back because it has the Social Security numbers of students and teachers on it.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| December 20, 2007 | **Greenville County School District**
Greenville, South Carolina | EDU | HACK | Unknown |

The district notified employees last week that its computers had been compromised and that employees' personal information was taken, including their names, home phone numbers and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| December 20, 2007 | **Watertown Public Schools**
Watertown, Massachusetts | EDU | PORT | 400 |

A laptop owned by Watertown was stolen from the vehicle of the Director or Personnel of Watertown Public Schools on December 18. There is a possibility that the laptop contained employee information. Employee names, Social Security numbers, addresses and other payroll information may have been exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 400

| December 18, 2007 | **Brownsville School District**
Brownsville, Pennsylvania | EDU | PHYS | Unknown |

Forms with employee personal information littered the fence of a Brownsville school district warehouse. Information on litter contained confidential letters with names, bank account numbers, and Social Security numbers. The forms may be more than ten years old, but they each contain information that's still valuable.

Information Source:
Media

records from this breach used in our total: 0

| December 4, 2007 | **Duke University**
Durham, North Carolina | EDU | HACK | 1,400 |

Social Security numbers of about 1,400 prospective law school applicants may have been compromised when a school Web site was

accessed illegally.

Information
Source: *records from this breach used in our total: 1,400*
Dataloss DB

November 21, 2007	**University of Florida** **Gainesville, Florida**	EDU	DISC	415

Those who suspect their Social Security numbers were posted can search their names on the Web site www.ssnbreach.org (http://www.ssnbreach.org) .

More than 400 former UF students might have been put at risk for identity theft after their Social Security numbers were posted on UF's Computing & Networking Services Web site. A news release from the Liberty Coalition, a group that works to preserve the privacy of individuals, said 14 files on the Web site contained sensitive information of 534 former UF students, including 415 Social Security numbers.

Information
Source: *records from this breach used in our total: 415*
Dataloss DB

November 20, 2007	**Beth Israel Deaconess Medical Center, Affiliated Physicians Group (APG)** **Foxborough, Massachusetts**	EDU	PHYS	53

On October 20, a briefcase was stolen from the vehicle of a physician. The briefcase contained patient encounter forms with names, addresses, Social Security numbers, telephone numbers and insurance information.

Information
Source: *records from this breach used in our total: 53*
Dataloss DB

November 16, 2007	**University of Wisconsin, Whitewater** **Whitewater, Wisconsin**	EDU	DISC	Unknown

Officials were notified by one individual about his ability to access an online search feature for the school's website. The search feature could be used to see student names and Social Security numbers along with some other limited student information. Access to the feature was promptly disabled upon notification of the problem.

Information
Source: *records from this breach used in our total: 0*
Media

November 16, 2007	**Wake Technical Community College** **Raleigh, North Carolina**	EDU	PORT	1,886

A flash drive that contained student names and Social Security numbers was lost and recovered. The flash drive was discovered missing on October 18 and was recovered within a month. The College stopped using Social Security numbers as student IDs shortly after this breach.

Information
Source: *records from this breach used in our total: 1,886*
Dataloss DB

November 14, 2007	**Harvard University** **Cambridge, Massachusetts**	EDU	PHYS	56

Folders containing information about students from the University's Division of Continuing Education were lost. The folders were from the previous year and included names, Social Security numbers, Harvard ID numbers, dates of birth, addresses, email addresses and phone numbers. Some of the folders contained additional information about the students and their dependents, spouses or parents. The information did not include credit card numbers. The University speculates that the folders were placed in a file cabinet that was later recycled.

Information
Source: *records from this breach used in our total: 56*

Dataloss DB

| November 2, 2007 | **Montana State University** **Bozeman, Montana** | EDU | PORT | 216 |

(406) 994-6550 http://eu.montana.edu/security (http://eu.montana.edu/security)

MSU learned that an employee's laptop computer had been stolen somewhere off-campus. It contained the Social Security numbers of 216 students and employees who lived in on-campus housing from 1998 to 2007.

Information Source:
Dataloss DB

records from this breach used in our total: 216

| November 2, 2007 | **Montana State University** **Bozeman, Montana** | EDU | DISC | 42 |

(406) 994-6550 http://eu.montana.edu/security (http://eu.montana.edu/security)

An independent security watchdog group informed MSU that an Excel spreadsheet with the names and Social Security numbers of 42 people, most of them hired in the summer of 2006, was publicly accessible on MSU's Web site.

Information Source:
Dataloss DB

records from this breach used in our total: 42

| November 2, 2007 | **Montana State University** **Bozeman, Montana** | EDU | DISC | 13 |

 (406) 994-6550, http://eu.montana.edu/security (http://eu.montana.edu/security)

While investigating that breach, MSU data-security staff found another Excel spreadsheet accidentally posted on the MSU Web site since 2002. It contained the Social Security numbers of 13 people who got travel vouchers from the computer science department in the College of Engineering.

Information Source:
Dataloss DB

records from this breach used in our total: 13

| November 1, 2007 | **City University of New York** **New York, New York** | EDU | PORT | 20,000 |

A broken laptop containing personal information was taken from the School's financial aid office.

Information Source:
Dataloss DB

records from this breach used in our total: 20,000

| October 30, 2007 | **University of Nevada, Reno** **Reno, Nevada** | EDU | PORT | 16,000 |

A University of Nevada, Reno administrative employee has lost a flash drive that contained the names and Social Security numbers of 16,000 current and former students.

Information Source:
Dataloss DB

records from this breach used in our total: 16,000

| October 29, 2007 | **New England School of Law** **Boston, Massachusetts** | EDU | DISC | 5,098 |

Personal information of alumni was available on the page of the School's website through a Google Internet search. The information included names, Social Security numbers, dates of birth, addresses and telephone numbers. The information was immediately removed from the website after the mid-October discovery.

Information Source:
Dataloss DB

records from this breach used in our total: 5,098

| October 25, 2007 | **University of Akron**
Akron, Ohio | EDU | PORT | 1,200 |

A microfilm containing the personal information of alumni were missing. Names, previous addresses, phone numbers, birth dates and Social Security numbers was on the missing microfilm.

Information Source:
Dataloss DB

records from this breach used in our total: 1,200

| October 23, 2007 | **Dixie State College**
St. George, Utah | EDU | DISC | 11,000 |

(866) 295-3033, idprotect@dixie.edu (mailto:idprotect@dixie.edu)

An unauthorized person reportedly gained access to a computer system and confidential files, including Social Security numbers, birth date information and addresses for some 11,000 alumni and current DSC employees who graduated or worked at DSC from 1986 to 2005.

Information Source:
Dataloss DB

records from this breach used in our total: 11,000

| October 23, 2007 | **Bates College**
Lewiston, Maine | EDU | DISC | 500 |

Two publicly accessible documents that contained the records of nearly 500 recipients of the federal Perkins Loan, along with each recipient's address, date of birth, Social Security number, legal name and loan amount, were accessible on the Bates network.

Information Source:
Dataloss DB

records from this breach used in our total: 500

| October 18, 2007 | **University of Cincinnati**
Cincinnati, Ohio | EDU | PORT | 7,000 |

The personal information of thousands of University of Cincinnati students and graduates has been stolen. A flash drive was taken from a UC employee last month. It contained the Social Security numbers and other data for more than 7,000 people.

Information Source:
Dataloss DB

records from this breach used in our total: 7,000

| October 17, 2007 | **Louisiana Office of Student Financial Assistance, Iron Mountain**
Baton Rouge, Louisiana | EDU | PORT | Unknown |

http://www.osfa.state.la.us/notice.htm (http://www.osfa.state.la.us/notice.htm)

Sensitive data for virtually all Louisiana college applicants and their parents over the past nine years were in a case lost last month during a move. The data included Social Security numbers for applicants and their parents. The bank account information for START account holders also was involved.

Information Source:
Dataloss DB

records from this breach used in our total: 0

October 13, 2007   **Montana State University**
Bozeman, Montana

EDU   HACK   1,400

(406) 994-6550, http://eu.montana.edu/security/ (http://eu.montana.edu/security/)

An unknown hacker remotely accessed a computer server that housed records containing credit card numbers and Social Security numbers of students who enrolled online for MSU Extended University courses during the last two years. The data in question was encrypted, and there is no evidence that personal information was stolen.

Information Source:
Dataloss DB

records from this breach used in our total: 1,400

October 9, 2007   **Pembroke Schools**
Pembroke, Massachusetts

EDU   DISC   Unknown

(781) 829-1178

Personal information on anyone who worked or volunteered for the Pembroke schools in the last four years was accessible via the Internet because of a weakness in the district's computer system. The information included names, birth dates and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

October 8, 2007   **University of Iowa**
Iowa City, Iowa

EDU   PORT   184

http://www.uiowa.edu/~phil/SSN.shtml (http://www.uiowa.edu/~phil/SSN.shtml)

A laptop computer was stolen from a former teaching assistant. The theft of the computer, which occurred last month in a break-in of the instructor's home, contained class records such as attendance, test scores, and grades of students who took his philosophy courses at the UI between 2002 and 2006. Social Security numbers were also present in 100 of the records.

Information Source:
Dataloss DB

records from this breach used in our total: 184

October 8, 2007   **Carnegie Mellon University**
Pittsburgh, Pennsylvania

EDU   PORT   Unknown

Two laptops were stolen from the office of a computer science professor. Both of the computers were believed to have contained significant personal identifying data, such as Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

September 19, 2007   **Kansas University**
Lawrence, Kansas

EDU   PHYS   Unknown

A number of documents containing Kansas University student, faculty and staff personal information were recovered from the recycling and trash in the Mathematics Department at Kansas University. The information included student exams, student change of grade forms, class rosters, copies of health insurance cards, copies of immigration forms as well as a copy of a Social Security card.

Information Source:

records from this breach used in our total: 0

Media

September 14, 2007	**Tennessee Tech University** **Cookeville, Tennessee**	EDU	DISC	3,100

Some 3,100 current or past students who owe the university money were notified today that some of their personal data may have been compromised. A technical problem in the way student bills are printed resulted in the chance that some student social security numbers and personal identification numbers may have been sent to another student's address.

Information Source: Dataloss DB

records from this breach used in our total: 3,100

September 14, 2007	**Cornell University** **Ithaca, New York**	EDU	STAT	12

A desktop computer was stolen from the East wing of Ives Hall in the School of Industrial and Labor Relations. It contained the names, Social Security numbers and dates of birth of some individuals.

Information Source: Dataloss DB

records from this breach used in our total: 12

September 10, 2007	**Purdue University** **West Lafayette, Indiana**	EDU	DISC	111

www.purdue.edu/news/coa0709.html (http://www.purdue.edu/news/coa0709.html) , (866) 275-1181

The university is warning those who were students in the fall of 2004 that information about them was inadvertently posted on the Internet. The information was in a document that contained the names and Social Security numbers of students in the Animal Sciences 102 class. The page was no longer in use but was on a computer server connected to the Internet. The document was found recently through an internal search and reported to the chief information security officer at Purdue.

Information Source: Dataloss DB

records from this breach used in our total: 111

September 9, 2007	**De Anza College** **Cupertino, California**	EDU	PORT	4,375

(408) 864-8292

Thousands of former students might be at risk for identity fraud after an instructor's laptop computer, containing students' personal information, was stolen last month. The computer contained the students' names, addresses, grades and in many cases Social Security numbers.

Information Source: Dataloss DB

records from this breach used in our total: 4,375

September 6, 2007	**University of South Carolina** **Columbia, South Carolina**	EDU	DISC	1,482

A number of files containing Social Security numbers, test scores and course grades were exposed online. It appears the person responsible for the breach may not have known enough about computers to realize the information could be accessed outside the university system.

Information Source: Dataloss DB

records from this breach used in our total: 1,482

September 4, 2007	**Brevard Public Schools** **Viera, Florida**	EDU	UNKN	61

A missing piece of luggage belonging to a state auditor contains the personal information of 61 Brevard Public Schools employees and had district personnel scrambling before the holiday weekend began to notify people that their names and Social Security numbers might be compromised.

UPDATE (9/21/07): Melbourne International Airport police arrested a 44-year-old defense subcontractor from California on charges of stealing luggage. He is in the Brevard County Jail, facing at least two charges of grand theft.

Information Source:
Media

records from this breach used in our total: 61

August 27, 2007	**University of Illinois** **Champaign-Urbana, Illinois**	EDU	DISC	5,247 Not added to total. It does not appear that SSNs or financial account numbers were exposed.

An e-mail sent Aug. 24 to about 700 University of Illinois engineering students contained a spreadsheet listing personal information, including addresses and grade point averages, of thousands of students. The spreadsheet attached to the mass mail did not contain Social Security numbers or the students' university identification numbers. But, the person who sent the mass e-mail attached a spreadsheet containing information on all 5,247 students in the College of Engineering. The spreadsheet included each student's name, e-mail address, major, gender, race and ethnicity, class, date admitted, spring 2007 grade point average, cumulative GPA, plus local address and phone number.

Information Source:
Media

records from this breach used in our total: 0

August 23, 2007	**Loomis Chaffee School** **Windsor, Connecticut**	EDU	UNKN	Unknown

Valuable computer equipment, including two large storage devices were stolen during a night time burglary from the locked IT facility on campus. The stolen storage devices contained information about some recent graduates of the school, including their names, Social Security numbers, and contact information from their days as students at the school.

Information Source:
Dataloss DB

records from this breach used in our total: 0

August 20, 2007	**University of Toledo** **Toledo, Ohio**	EDU	PORT	Unknown

A laptop computer has been stolen from an office in the Student Recreation Center that contained some student and employee names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

August 17, 2007	**University of New Hampshire** **Durham, New Hampshire**	EDU	DISC	29

An MS Excel spreadsheet containing names and Social Security numbers of graduate students at the University was posted within the University's website on or around April 17, 2007. Specifically, the spreadsheet contained the credit hour and tuition information associated with "inter-college" graduate programs. In addition to the credit hour and tuition information that were visible at the top of the spreadsheet, the bottom of the report also included the names and Social Security numbers of students. A staff member recognized the mistake on July 27.

Information Source:
Dataloss DB

records from this breach used in our total: 29

| August 10, 2007 | **Loyola University**
Chicago, Illinois | EDU | STAT | 5,800 |

A computer with the Social Security numbers of 58 hundred students was discarded before its hard drive was erased, forcing the school to warn students about potential identify theft.

Information Source:
Dataloss DB

records from this breach used in our total: 5,800

| August 8, 2007 | **Yale University**
New Haven, Connecticut | EDU | STAT | 10,200 |

Social Security numbers for over 10,000 current and former students, faculty and staff were compromised last month following the theft of two University computers

Information Source:
Dataloss DB

records from this breach used in our total: 10,200

| August 2, 2007 | **University of Toledo**
Toledo, Ohio | EDU | STAT | Unknown |

(419) 530-4836, (419) 530-3661, (419) 530-1472

Two computers were stolen with hard drives containing student and staff Social Security numbers, names, and grade change information.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| July 26, 2007 | **United States Marine Corps, Penn State University**
Harrisburg, Pennsylvania | EDU | DISC | 10,554 |

Data belonging to 10,554 Marines was "improperly posted" by Penn State University, according to the Marine Corps. Names and Social Security numbers of Marines could be found via Google search engine. Penn State University was under a research contract with the Marine Corps.

Information Source:
Dataloss DB

records from this breach used in our total: 10,554

| July 21, 2007 | **University of Michigan**
Ann Arbor, Michigan | EDU | HACK | 5,500 |

University databases were hacked. Names, addresses, Social Security numbers, birth dates, and in some cases, the school districts where former students were teaching were exposed.

Information Source:

records from this breach used in our total: 5,500

Dataloss DB

| July 19, 2007 | **Jackson Local Schools**
Massillon, Ohio | EDU | DISC | 1,800 |

The Social Security numbers of present and former Jackson Local Schools' employees were at risk of public access on a county maintained Web site.

Information Source:
Dataloss DB

records from this breach used in our total: 1,800

| July 18, 2007 | **Purdue University**
West Lafayette, Indiana | EDU | DISC | 50 |

(866) 605-0013

Files which were no longer in use were discovered on a computer server connected to the Internet. The files contained names and Social Security numbers of students who were enrolled in an industrial engineering course in spring 2002 or fall 2004.

Information Source:
Dataloss DB

records from this breach used in our total: 50

| July 15, 2007 | **Westminster College**
Salt Lake City, Utah | EDU | DISC | 100 |

Names of students, former and current were printed in two files along with each student's Social Security number. The files were on a student Web server used by Westminster students.

Information Source:
Media

records from this breach used in our total: 100

| July 11, 2007 | **Texas A&M University**
Corpus Christi, Texas | EDU | PHYS | 49 |

College of Business officials are investigating a faculty member for the misplacement of a business law class roster containing the names and Social Security numbers of students.

Information Source:
Media

records from this breach used in our total: 49

| July 5, 2007 | **Highland University**
Las Vegas, New Mexico | EDU | UNKN | 420 |

A building on the campus had been broken into, and the affected offices might have contained such personal information as Social Security numbers, credit card and bank account information.

Information Source:
Dataloss DB

records from this breach used in our total: 420

| June 29, 2007 | **Harrison County Schools**
Charleston, West Virginia | EDU | STAT | Unknown |

Several computers that contained the personal information, including Social Security numbers, of several Harrison County school employees were stolen. Workers Comp claims between January of 2001 and February of 2007 are at risk.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| June 27, 2007 | **Bowling Green State University**
Bowling Green, Ohio | EDU | PORT | 199 |

Lost storage device contained Social Security numbers, and names of 199 former students.

Information Source:
Dataloss DB

records from this breach used in our total: 199

| June 27, 2007 | **University of California, Davis**
Davis, California | EDU | HACK | 1,120 |

deansoffice@vetmed.ucdavis.edu (mailto:deansoffice@vetmed.ucdavis.edu)

Computer-security safeguards were breached. Compromised information included the applicants' names, birth dates and, in most cases, Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 1,120

| June 18, 2007 | **Shamokin Area School District**
Coal Township, Pennsylvania | EDU | DISC | Unknown |

A local newspaper employee gained unauthorized access to the Shamokin Area School District's computer database. It is the same system that stores students' personal information, including Social Security numbers. That newspaper employee brought the security flaw to the attention of school officials.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| June 18, 2007 | **Texas A&M University**
Corpus Christi, Texas | EDU | PORT | 8,000 |

A professor vacationing off the coast of Africa took data with him on a small computer storage device which was lost or stolen. It is thought to contains SSNs and dates of birth for students enrolled in the spring, summer and fall semesters of 2006

Information Source:
Dataloss DB

records from this breach used in our total: 8,000

| June 14, 2007 | **Georgia Tech University**
Atlanta, Georgia | EDU | DISC | 23,000 Not included in Total because it's not clear SSNs or account numbers were exposed. |

An electronic file containing the personal information of current and former Georgia Tech students was exposed briefly.

Information Source:

records from this breach used in our total: 0

Dataloss DB

| June 11, 2007 | **Grand Valley State University**
Allendale, Michigan | EDU | PORT | 3,000 |

Jann Joseph (616) 331-2110

A flash drive containing confidential information was stolen. Social Security numbers of current and former students were on the flash drive, stolen from the English department.

Information Source:
Dataloss DB

records from this breach used in our total: 3,000

| June 8, 2007 | **University of Virginia**
Charlottesville, Virginia | EDU | HACK | 5,735 |

http://www.virginia.edu/uvatoday/newsRelease.php?id=2217 (http://www.virginia.edu/uvatoday/newsRelease.php?id=2217) , identity-assistance@virginia.edu (mailto:identity-assistance@virginia.edu) , (866) 621-5948

A breach in one of the computer applications resulted in exposure of sensitive information belonging to current and former U.Va. faculty members. The information included names, Social Security numbers and dates of birth. The investigation has revealed that on 54 separate days between May 20, 2005, and April 19, 2007, hackers tapped into the records of 5,735 faculty members.

Information Source:
Dataloss DB

records from this breach used in our total: 5,735

| June 8, 2007 | **University of Iowa**
Iowa City, Iowa | EDU | HACK | 1,100 |

Social Security numbers of faculty, students and prospective students were stored on the Web database program that was compromised.

Information Source:
Dataloss DB

records from this breach used in our total: 1,100

| June 6, 2007 | **Cedarburg High School**
Cedarburg, Wisconsin | EDU | DISC | Unknown |

Students obtained names, addresses and Social Security numbers and might have accessed personal bank account information of current and former district employees.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| June 3, 2007 | **Gadsden State Community College**
College Gadsden, Alabama | EDU | PHYS | 400 |

Students who took an Art Appreciation class at the Ayers Campus between 2005 and 2006 had their names, grades and Social Security numbers scattered across a local business' driveway.

Information Source:
Dataloss DB

records from this breach used in our total: 400

| May 23, 2007 | **Waco Independent School District**
Waco, Texas | EDU | HACK | 17,400 |

Two high school seniors recently hacked into the district's computer network potentially compromising the personal information including Social Security numbers of students and employees.

Information Source:
Dataloss DB

records from this breach used in our total: 17,400

| May 22, 2007 | **University of Colorado, Boulder**
Boulder, Colorado | EDU | HACK | 45,000 |

 Hotline: (303) 492-1655

A hacker launched a worm that attacked a University computer server used by the College of Arts and Sciences. Information for 45,000 students enrolled at UC-B from 2002 to the present was exposed, including SSNs. The breach was discovered May 12. Apparently anti-virus software had not been properly configured.

Information Source:
Dataloss DB

records from this breach used in our total: 45,000

| May 20, 2007 | **Northwestern University**
Chicago, Illinois | EDU | PORT | Unknown |

A laptop belonging to the financial aid office was stolen. It contained SSNs and other information of some alumni.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 19, 2007 | **Stony Brook University**
Stony Brook, New York | EDU | DISC | 90,000 |

http://www.stonybrook.edu/sb/disclosure/ (http://www.stonybrook.edu/sb/disclosure/) , Call Center, (866) 645-5830 (available until July 15, 2007)

SSNs and university ID numbers of faculty, staff, students, alumni, and other community members were visible via the Google search engine after they were posted to a Health Sciences Library Web server April 11. It was discovered and removed 2 weeks later.

Information Source:
Dataloss DB

records from this breach used in our total: 90,000

| May 18, 2007 | **Yuma Elementary School District No. 1**
Yuma, Arizona | EDU | PHYS | 91 |

SSNs of 91 substitute teachers were stolen May 7 when a district employee's car was broken into and a brief case was taken containing payroll reports. The reports did not include bank account information..

Information Source:
Dataloss DB

records from this breach used in our total: 91

| May 18, 2007 | **Indianapolis Public Schools**
Indianapolis, Indiana | EDU | DISC | 7,500 (No SSNs or financial information reported) |

A local newspaper reporter discovered that sensitive personal information was accessible online, including employee performance reviews,

student grade books, student special education needs, and essays.

Information Source: Dataloss DB

records from this breach used in our total: 0

May 14, 2007 | **Community College of Southern Nevada**
North Las Vegas, Nevada | EDU | HACK | 197,000

A virus attacked a computer server and could have allowed a hacker to access students' personal information including names, Social Security numbers and dates of birth, but the school is not certain whether anything was actually stolen from the school's computer system.

Information Source: Dataloss DB

records from this breach used in our total: 197,000

May 12, 2007 | **Goshen College**
Goshen, Indiana | EDU | HACK | 7,300

http://www.goshen.edu/news/pressarchive/05-11-07-security.html (http://www.goshen.edu/news/pressarchive/05-11-07-security.html) ,
info@goshen.edu (mailto:info@goshen.edu) , (866) 877-3055

A hacker accessed a college computer that contained the names, addresses, birth dates, Social Security numbers and phone numbers of students and information on some parents with the suspected motivation of using the system to send spam e-mails.

Information Source: Dataloss DB

records from this breach used in our total: 7,300

May 8, 2007 | **University of Missouri**
Columbia, Missouri | EDU | HACK | 22,396

(866) 241-5619

A hacker accessed a computer database containing the names and Social Security numbers of employees of any campus within the University system in 2004 who were also current or former students of the Columbia campus.

Information Source: Dataloss DB

records from this breach used in our total: 22,396

May 8, 2007 | **Jones Beauty College**
Dallas, Texas | EDU | PHYS | Unknown

The Texas Attorney General filed an enforcement action against the College in March. Student financial aid forms with Social Security numbers and other personal information had been improperly discarded.

Information Source: Media

records from this breach used in our total: 0

May 3, 2007 | **Louisiana State University, E..J. Ourso College of Business**
Baton Rogue, Louisiana | EDU | PORT | 750

A laptop stolen from a faculty member's home contained personally identifiable information including may have included students' Social Security numbers, full names and grades of University students.

Information Source: Dataloss DB

records from this breach used in our total: 750

| May 3, 2007 | **Montgomery College**
Conroe, Texas | EDU | DISC | Unknown |

A new employee posted the personal information of all graduating seniors including names, addresses and Social Security numbers on a computer drive that is publicly accessible on all campus computers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 29, 2007 | **University of New Mexico**
Alburquerque, New Mexico | EDU | PORT | 3,000 not included in total below because SSNs were apparently not compromised) |

Employees' personal information including names, e-mail and home addresses, UNM ID numbers and net pay for a pay period for staff, faculty and a few graduate students may have been stored on a laptop computer stolen from the San Francisco office of an outside consultant working on UNM's human resource and payroll systems.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| April 24, 2007 | **Purdue University**
West Lafayette, Indiana | EDU | DISC | 175 |

(866) 307-8513

Personal information including names and Social Security numbers of students who were enrolled in a freshman engineering honors course was on a computer server connected to the Internet that had been indexed by Internet search engines and consequently was available to individuals searching the Web.

Information Source:
Dataloss DB

records from this breach used in our total: 175

| April 19, 2007 | **New Mexico State University**
Las Cruces, New Mexico | EDU | DISC | 5,600 |

The names and Social Security numbers of students who registered online to attend their commencement ceremonies from 2003 to 2005 were accidentally posted on the school's Web site when an automated program moved what was supposed to be a private file into a public section of the Web site.

Information Source:
Dataloss DB

records from this breach used in our total: 5,600

| April 18, 2007 | **Ohio State University**
Columbus, Ohio | EDU | HACK | 14,000 |

http://www.osu.edu/news/newsitem1673 (http://www.osu.edu/news/newsitem1673)

A hacker accessed the names, Social Security numbers, employee ID numbers and birth dates of 14,000 current and former staff members.

Information

Source:
Dataloss DB

records from this breach used in our total: 14,000

| April 18, 2007 | **University of California, San Francisco (UCSF)**
San Francisco, California | EDU | STAT | 3,000 |

(866) 485-8777, http://news.ucsf.edu/releases/ucsf-computer-server-with-research-subject-information-is-stolen/ (http://news.ucsf.edu/releases/ucsf-computer-server-with-research-subject-information-is-stolen/) , http://security.ucsf.edu/alert/information.html (http://security.ucsf.edu/alert/information.html)

A computer file server containing names, contact information, and Social Security numbers for study subjects and potential study subjects related to research on causes and cures for different types of cancer was stolen from a locked UCSF office. For some individuals, the files also included personal health information.

Information
Source:
Dataloss DB

records from this breach used in our total: 3,000

| April 18, 2007 | **Ohio State University**
Columbus, Ohio | EDU | PORT | 3,500 |

http://www.osu.edu/news/newsitem1673 (http://www.osu.edu/news/newsitem1673)

The names, Social Security numbers and grades of 3,500 former chemistry students were on class rosters housed on two laptop computers stolen from a professor's home in late February.

Information
Source:
Dataloss DB

records from this breach used in our total: 3,500

| April 11, 2007 | **Black Hills State University**
Spearfish, South Dakota | EDU | STAT | 56 |

http://www.bhsu.edu/AboutBHSU/NewsEvents/tabid/3454/articleType/ArticleView/articleId/339/Default.aspx (http://www.bhsu.edu/AboutBHSU/NewsEvents/tabid/3454/articleType/ArticleView/articleId/339/Default.aspx) , (605) 642-6215

Names and Social Security numbers of scholarship winners were inadvertently posted and publicly available on the university's web site.

Information
Source:
Dataloss DB

records from this breach used in our total: 56

| April 6, 2007 | **Chicago Public Schools**
Chicago, Illinois | EDU | PORT | 40,000 |

(773) 553-1142

Two laptop computers contain the names and Social Security numbers of current and former employees was stolen from Chicago Public Schools headquarters.

Information
Source:
Dataloss DB

records from this breach used in our total: 40,000

| April 4, 2007 | **University of California, San Francisco (UCSF)**
San Francisco, California | EDU | HACK | 46,000 |

(415) 353-8100, isecurity@ucsf.edu (mailto:isecurity@ucsf.edu)

An unauthorized party may have accessed the personal information including names, Social Security numbers, and bank account numbers

of students, faculty, and staff associated with UCSF or UCSF Medical Center over the past two years by compromising the security of a campus server.

Information Source:
Dataloss DB

records from this breach used in our total: 46,000

April 4, 2007	**Guilford Technical Community College** **Greensboro, North Carolina**	EDU	PHYS	550 (No SSNs or financial information reported)

A surplus file cabinet that was temporarily stored in a warehouse area prior to an auction held sensitive paper documents. Anyone entering the warehouse could have viewed or taken the files.

Information Source:
Dataloss DB

records from this breach used in our total: 0

March 30, 2007	**University of Montana Western** **Dillon, Montana**	EDU	PORT	400

A computer disk containing students' Social Security numbers, names, birth dates, addresses and other personal information was stolen from a professor's office. The stolen information belonged to over 400 students enrolled in the TRIO Student Support Services program, which offers financial and personal counseling and other assistance.

Information Source:
Dataloss DB

records from this breach used in our total: 400

March 27, 2007	**St. Mary Parish Schools** **Centerville, Louisiana**	EDU	DISC	380

Personal information including Social Security numbers of St. Mary Parish public school employees was available on the Internet when a Yahoo!Web crawler infiltrated the server of the school's technology department.

Information Source:
Dataloss DB

records from this breach used in our total: 380

March 23, 2007	**New York Institute of Technology** **Old Westbury, New York**	EDU	DISC	256

A file with the names, Social Security numbers, addresses, dates of birth, degree types and majors of former NYIT students was posted on NYIT's website. The information was not accessible via the NYIT website, but could be found through an Internet search.

Information Source:
Dataloss DB

records from this breach used in our total: 256

March 16, 2007	**Springfield City Schools, Ohio State Auditor** **Springfield, Ohio**	EDU	PORT	1,950

http://www.spr.k12.oh.us/ (http://www.spr.k12.oh.us/) , http://www.spr.k12.oh.us./ourboard/treasdocs/notificationofDataTheft.pdf (http://www.spr.k12.oh.us./ourboard/treasdocs/notificationofDataTheft.pdf)

A laptop containing personal information of current and former employees of Springfield City Schools including their names and Social Security numbers was stolen from a state auditor employee's vehicle while parked at home in a garage.

Information Source:
Dataloss DB

records from this breach used in our total: 1,950

| March 10, 2007 | **University of Idaho**
Moscow, Idaho | EDU | DISC | 2,700 |

888-900-3783

A data file posted to the school's Web site contained personal information including names, birthdates and Social Security numbers of University employees.

Information Source:
Dataloss DB

records from this breach used in our total: 2,700

| March 7, 2007 | **Los Rios Community College**
Sacramento, California | EDU | DISC | 2,000 |

Student information including Social Security numbers were accessible on the Internet after the school used actual data to test a new online application process in October.

Information Source:
Dataloss DB

records from this breach used in our total: 2,000

| March 3, 2007 | **Metropolitan State College of Denver**
Denver, Colorado | EDU | PORT | 988 |

http://www.mscd.edu/securityalert/ (http://www.mscd.edu/securityalert/) , 866-737-6622

A faculty member's laptop computer that contained the names and Social Security numbers of former students was stolen from its docking station on campus.

Information Source:
Dataloss DB

records from this breach used in our total: 988

| February 21, 2007 | **Georgia Institute of Technology**
Atlanta, Georgia | EDU | HACK | 3,000 |

404-894-2499, hr@gatech.edu (mailto:hr@gatech.edu)

Personal information of former employees mostly in the School of Electrical and Computer Engineering including name, address, Social Security number, other sensitive information, and about 400 state purchasing card numbers, were compromised by unauthorized access to a Georgia Tech computer account.

Information Source:
Dataloss DB

records from this breach used in our total: 3,000

| February 19, 2007 | **Clarksville-Montgomery County middle and high schools**
Clarksville, Tennessee | EDU | DISC | 633 |

Staff and faculty Social Security numbers, used as employee identification numbers, were embedded in file photos by the company that took yearbook pictures and inadvertently placed in a search engine on school system's Web site.

Information Source:
Dataloss DB

records from this breach used in our total: 633

| February 15, 2007 | **City College of San Francisco**
San Francisco, California | EDU | DISC | 11,000 students |

 (800) 436-0108, www.ccsf.edu/securityalert (http://www.ccsf.edu/securityalert)

Names, grades, and SSNs were posted on an unprotected Web site after summer session in 1999. CCSF stopped using SSNs as studens IDs in 2002.

Information Source:
Dataloss DB

records from this breach used in our total: 11,000

| February 15, 2007 | **The Professional Education Institute**
Burr Ridge, Illinois | EDU | DISC | 34 |

Customer information was accidentally exposed online because of a data encryption lapse. The Social Security numbers and dates of birth of some customers were viewable on the Millionaire Elite Website. Two New Hampshire, three Maine and 29 New York residents were affected by the breach. The total number of individuals affected nationwide was not revealed.

Information Source:
Dataloss DB

records from this breach used in our total: 34

| February 9, 2007 | **East Carolina University**
Greenville, North Carolina | EDU | DISC | 65,000 students, alumni, and staff members |

http://www.ecu.edu/incident/ (http://www.ecu.edu/incident/) , 877-328-6660

A programming error resulted in personal information of 65,000 individuals being exposed on the University's Web site. The data has since been removed. Included were names, addresses, SSNs, and in some cases credit card numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 65,000

| February 9, 2007 | **Radford University, Waldron School of Health and Human Services**
Radford, Virginia | EDU | HACK | 2,400 children |

A computer security breach exposed the personal information, including SSNs, of children enrolled in the FAMIS program, Family Access to Medical Insurance Security.

Information Source:
Dataloss DB

records from this breach used in our total: 2,400

| February 7, 2007 | **University of Nebraska**
Lincoln, Nebraska | EDU | DISC | 72 |

An employee accidentally posted SSNs of 72 students, professors, and staff on UNL's public Web site where they remained for 2 years. They have since been removed.

Information Source:
Dataloss DB

records from this breach used in our total: 72

| February 7, 2007 | **Central Connecticut State University**
New Britain, Connecticut | EDU | DISC | 750 students |

Social Security numbers of about 750 CCSU students were exposed in the name and address window on envelopes mailed to them. The envelopes were not folded correctly. They contained IRS 1098T forms.

Information Source:
Dataloss DB

records from this breach used in our total: 750

| February 2, 2007 | **University of Missouri, Research Board Grant Application System**
Columbia, Missouri | EDU | HACK | 1,220 |

A hacker broke into a UM computer server mid-January and might have accessed personal information, including SSNs, of 1,220 researchers on 4 campuses. The passwords of 2,579 individuals might also have been exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 1,220

| January 29, 2007 | **Mendoza College of Business, Notre Dame University**
Notre Dame, Indiana | EDU | DISC | Unknown |

Additional location: South Bend, Indiana

A file of individuals who took the GMAT test (Graduate Management Admissions Test) was mistakenly left on a computer that was decommissioned. The computer was later reactivated and plugged into the Internet. Its files were available through a file-sharing program. Data included names, scores, SSNs and demographic information from 2001.

Information Source:
Media

records from this breach used in our total: 0

| January 28, 2007 | **New York Academy of Medicine**
New York, New York | EDU | STAT | 7,460 (0 complete SSNs) |

A computer was stolen during an office burglary in October 28. The last four digits of research participants' Social Security numbers, full names and dates of birth were on a database on the computer. Some participants also had their addresses and laboratory data exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| January 26, 2007 | **Vanguard University**
Costa Mesa, California | EDU | STAT | 5,105 financial aid applicants |

(800) 920-7312

On Jan. 16, 2 computers were discovered stolen from the financial aid office. Data included names, SSNs, dates of birth, phone numbers, driver's license numbers, and lists of assets. Affected financial aid applicants from 2005-2006 and 2006-2007 school years.

Information Source:
Dataloss DB

records from this breach used in our total: 5,105

1,400

| January 26, 2007 | **Eastern Illinois University** **Charleston, Illinois** | EDU | STAT | currently enrolled students |

A desktop computer was stolen from the Student Life office containing membership rosters -- including SSNs, birthdates, and addresses -- of the University's 23 fraternities and sororities. A hard drive and memory from 2 other computers were also stolen.

Information Source: Dataloss DB

records from this breach used in our total: 1,400

| January 25, 2007 | **Clay High School** **Oregon, Ohio** | EDU | HACK | Unknown |

A former high school student obtained sensitive staff and student information through an apparent security breach. The data was copied onto an iPod and included names, birth dates, SSNs, addresses, and phone numbers.

Information Source: Dataloss DB

records from this breach used in our total: 0

| January 24, 2007 | **Cornell University** **Detroit, Michigan** | EDU | PORT | 122 |

An employee laptop was lost after being checked as baggage at Detroit Metropolitan International Airport. It contained names, Social Security numbers and credit card numbers of some people.

Information Source: Dataloss DB

records from this breach used in our total: 122

| January 23, 2007 | **Rutgers-Newark University, Political Science Department** **Newark, New Jersey** | EDU | PORT | 200 students |

An associate professor's laptop was stolen, containing names and SSNs of 200 students. Rutgers no longer uses SSNs as student IDs, but student IDs from past years are still SSNs.

Information Source: Dataloss DB

records from this breach used in our total: 200

| January 20, 2007 | **Greenville South Carolina County School District** **Greenville, South Carolina** | EDU | PHYS | Unknown |

Boxes of personnel records were inadvertently left unsecured during renovations. Ten boxes held the names and Social Security numbers of teachers employed by the district between 1972 and 1990. Other boxes contained personnel records through 1998. District officials secured the boxes after receiving an anonymous call about the mistake.

Information Source: Dataloss DB

records from this breach used in our total: 0

| January 16, 2007 | **University of New Mexico** **Albuquerque, New Mexico** | EDU | STAT | Unknown |

At least 3 computers and 4 monitors were stolen from the associate provost's office overnight between Jan. 2 and 3. They may have included faculty members' names and SSNs.

Information

Source:
Dataloss DB

records from this breach used in our total: 0

| January 11, 2007 | **University of Idaho**
Moscow, Idaho | EDU | STAT | 70,000 |

(866) 351-1860

Over Thanksgiving weekend, 3 desktop computers were stolen from the Advancement Services office containing personal information of alumni, donors, employees, and students. 331,000 individuals may have been exposed, with as many as 70,000 records containing SSNs, names and addresses.

Information
Source:
Dataloss DB

records from this breach used in our total: 70,000

| January 10, 2007 | **University of Arizona**
Tucson, Arizona | EDU | UNKN | Unknown |

Breaches occurred in November and December 2006 that affected services with UA Student Unions, University Library, and UA Procurement and Contracting Services. Some services were shut down for several days.

Information
Source:
Dataloss DB

records from this breach used in our total: 0

| January 3, 2007 | **Academic Magnet High School**
North Charleston, South Carolina | EDU | PORT | 500 (No SSNs or financial information reported) |

A recent burglary makes it the third time that computers were stolen during campus burglaries. Two other incidents occurred in November. Student information was on the laptop stolen in the recent burglary. School officials felt that risk of identity theft was extremely low because the information was password protected and encrypted.

Information
Source:
Dataloss DB

records from this breach used in our total: 0

| January 2, 2007 | **Notre Dame University**
Notre Dame, Indiana | EDU | PORT | Unknown |

Additional location: South Bend, IN

A University Director's laptop was stolen before Christmas. It contained personal information of employees, including names, SSNs, and salary information.

Information
Source:
Dataloss DB

records from this breach used in our total: 0

| December 27, 2006 | **Montana State University**
Bozeman, Montana | EDU | DISC | 259 |

A student working in the loan office mistakenly sent packets containing lists of student names, Social Security numbers, and loan information to other students.

Information

Source:
Dataloss DB

records from this breach used in our total: 259

| December 22, 2006 | **Texas Woman's University**
Dallas, Texas | | EDU | DISC | 15,000 students |

Additional locations: Denton and Houston, TX

A document containing names, addresses and SSNs of 15,000 TWU students was transmitted over a non-secure connection.

Information Source:
Media

records from this breach used in our total: 15,000

| December 22, 2006 | **Utah Valley State College**
Orem, Utah | | EDU | DISC | 15,000 |

Social Security numbers and other personal information of students and faculty was accessible via Yahoo's search engine. The information was removed from UVSC's servers. Some Distance Education instructors and some students enrolled in UVSC courses between January 2002 and January 2005 were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 15,000

| December 21, 2006 | **Hunter College of the City University of New York**
New York, New York | | EDU | DISC | 140 |

The full names and Social Security numbers of certain individuals were on a spreadsheet that an employee emailed to a group of students on November 8. Students were instructed to delete the file after the discovery. At least 140 New York residents were affected, but the total number of people affected nationwide was not revealed.

Information Source:
Dataloss DB

records from this breach used in our total: 140

| December 21, 2006 | **Wake County Public School System**
Raleigh, North Carolina | | EDU | PORT | 3,396 |

A flash drive that contained employee names and Social Security numbers was misplaced. The flash drive was found two days later.

Information Source:
Dataloss DB

records from this breach used in our total: 3,396

| December 21, 2006 | **City University of New York**
New York, New York | | EDU | DISC | 96 |

Confidential data from the University server was accidentally made available through a Google search. The error was discovered on October 17 and faculty, students and staff were affected. The information included full names, Social Security numbers, dates of birth, addresses, email addresses and University library identification card numbers. The copy of the file was removed from Google on October 20.

Information Source:
Dataloss DB

records from this breach used in our total: 96

| December 20, 2006 | **Big Foot High School**
Walworth, Wisconsin | | EDU | DISC | 87 |

Personal information was accidentally exposed on the High School's Web site for a short time, perhaps for about 36 minutes, according to a report. Information included last names, SSNs, and birthdates. Current and former employees were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 87

| December 19, 2006 | **Mississippi State University**
Jackson, Mississippi | EDU | DISC | 2,400 students and emploNlees |

SSNs and other personal information were inadvertently posted on a publicly accessible MSU Web site. The breach was discovered last week and the information has since been removed.

Information Source:
Dataloss DB

records from this breach used in our total: 2,400

| December 15, 2006 | **University of Colorado, Boulder, Academic Advising Center**
Boulder, Colorado | EDU | HACK | 17,500 |

http://www.colorado.edu/its/security/awareness/privacy/identitytheft.pdf
(http://www.colorado.edu/its/security/awareness/privacy/identitytheft.pdf)

A server in the Academic Advising Center was the subject of a hacking attack. Personal information exposed included names and SSNs for individuals who attended orientation sessions from 2002-2004. CU-Boulder has since ceased using SSNs as identifiers for students, faculty, staff, and administrators.

Information Source:
Dataloss DB

records from this breach used in our total: 17,500

| December 15, 2006 | **City University of New York**
New York, New York | EDU | STAT | 445 |

Two computers were stolen from the York Support Services office. The computers contained databases including full names, Social security numbers and dates of birth.

Information Source:
Dataloss DB

records from this breach used in our total: 445

| December 14, 2006 | **St. Vrain Valley School District**
Longmont, Colorado | EDU | PHYS | 600 students |

Paper records containing student information were stolen, along with a laptop, from a nurse's car Nov. 20. Personal information included students' names, dates of birth, names of their schools, what grade they are in, their Medicaid numbers (presumably SSNs), and their parents' names. The laptop contained no personal data.

Information Source:
Dataloss DB

records from this breach used in our total: 600

| December 14, 2006 | **Riverside High School**
Durham, North Carolina | EDU | DISC | Thousands of school employees (at least 2,000) |

Two students discovered a breach in the security of a Durham Public Schools computer as part of a class assignment. They reported to school officials that they were able to access a database containing SSNs and other personal information of thousands of school employees. The home of one student was searched by Sheriff's deputies and the family computer was seized.

Information Source: Dataloss DB

records from this breach used in our total: 2,000

| December 12, 2006 | **University of California at Los Angeles (UCLA)**
Los Angeles, California | EDU | HACK | 800,000 |

Affected individuals can call UCLA at (877) 533-8082, http://www.identityalert.ucla.edu (http://www.identityalert.ucla.edu)

Hacker(s) gained access to a UCLA database containing personal information on current and former students, current and former faculty and staff, parents of financial aid applicants, and student applicants, including those who did not attend. Exposed records contained names, SSNs, birth dates, home addresses, and contact information. About 3,200 of those notified are current or former staff and faculty of UC Merced and current and former staff of UC's Oakland headquarters.

Information Source: Media

records from this breach used in our total: 800,000

| December 12, 2006 | **University of Texas, Dallas**
Dallas, Texas | EDU | HACK | 35,000 |

Affected individuals can call (972) 883-4325, http://www.utdallas.edu/datacompromise/form.html (http://www.utdallas.edu/datacompromise/form.html)

The University discovered that personal information of current and former students, faculty members, and staff may have been exposed by a computer network intrusion -- including names, SSNs, home addresses, phone numbers and e-mail addresses.

UPDATE (12/14/06): The number of people affected was first thought to be 5,000, but was increased to 6,000.

UPDATE (01/19/07): Officials now say 35,000 individuals may have been exposed.

Information Source: Dataloss DB

records from this breach used in our total: 35,000

| December 9, 2006 | **Virginia Commonwealth University (VCU)**
Richmond, Virginia | EDU | DISC | 561 students |

Personal information of 561 students was inadvertently sent as attachments on Nov. 20 in an e-mail, including names, SSNs, local and permanent addresses and grade-point averages. The e-mail was sent to 195 students to inform them of their eligibility for scholarships.

Information Source: Dataloss DB

records from this breach used in our total: 561

| December 7, 2006 | **Cornell University**
Ithica, New York | EDU | PORT | 210 |

A laptop was stolen from an employee. Names and Social Security numbers were on the computer.

Information Source: Dataloss DB

records from this breach used in our total: 210

| December 5, 2006 | **Nassau Community College**
Garden City, New York | EDU | PHYS | 21,000 |

A printout is missing that contains information about each of NCC's 21,000 students, including names, SSNs, addresses, and phone numbers. It disappeared from a desk in the Student Activities Office.

Information Source:
Dataloss DB

records from this breach used in our total: 21,000

November 28, 2006	**California State University, Los Angeles (Cal State LA), Charter College of Education** **Los Angeles, California**	EDU	PORT	2,534

(800) 883-4029

An employee's USB drive was inside a purse stolen from a car trunk. It contained personal information on 48 faculty members and more than 2,500 students and applicants of a teacher credentialing program. Information included names, SSNs, campus ID numbers, phone numbers, and e-mail addresses.

Information Source:
Dataloss DB

records from this breach used in our total: 2,534

November 27, 2006	**Greenville County School District** **Greenville, South Carolina**	EDU	STAT	At least 101,000 students and employees

School district computers sold to the WH Group at auctions between 1999 and early 2006 contained the birth dates, SSNs, driver's license numbers and Department of Juvenile Justice records of approximately 100,000 students. The computers also held sensitive data for more than 1,000 school district employees.

UPDATE(12/10/06): A judge ordered the WH Group to return the computers and the confidential data on them to the school district.

Information Source:
Dataloss DB

records from this breach used in our total: 101,000

November 27, 2006	**Chicago Public Schools via All Printing & Graphics, Inc.** **Chicago, Illinois**	EDU	DISC	1,740 former Chicago Public School employees

A company hired to print and mail health insurance information to former Chicago Public School employees mistakenly included a list of the names, addresses and SSNs of the nearly 1,740 people receiving the mailing. Each received the 125-page list of the 1,740 former employees.

Information Source:
Dataloss DB

records from this breach used in our total: 1,740

November 17, 2006	**Jefferson College of Health Sciences** **Roanoke, Virginia**	EDU	DISC	143

An email containing the names and SSNs of 143 students intended for one employee was inadvertently sent to the entire student body of 900.

Information Source:
Dataloss DB

records from this breach used in our total: 143

November 15,	**Stony Brook University**	EDU	

| 2006 | **Stony Brook, New York** | | STAT | 2,000 |

A computer stolen on August 15 contained names and Social Security numbers. People involved in the Professional Teachers Program were affected. An employee of a moving company used by the University is believed to be responsible for the theft. The computer was returned on October 6 and was used by unauthorized persons during its absence.

Information Source:
Dataloss DB

records from this breach used in our total: 2,000

| November 13, 2006 | **Connors State College**
Warner, Oklahoma | EDU | PORT | Considerably more than 22,500 |

(918) 463-6267, perline@connorsstate.edu (mailto:perline@connorsstate.edu)

On Oct. 15, a laptop computer was discovered stolen from the college. (It has since been recovered by law enforcement). The computer contains Social Security numbers and other data for Connors students plus 22,500 high school graduates who qualify for the Oklahoma Higher Learning Access Program scholarships.

Information Source:
Dataloss DB

records from this breach used in our total: 22,500

| November 10, 2006 | **NYS Higher Education Services**
Albany, New York | EDU | PHYS | 49 |

Paper documents were lost when the package containing them was damaged by a carrier's mechanical equipment. The documents may have been thrown away by the carrier. The information on the documents included name, Social Security number and address. At least 49 New York residents were affected, but the total number of people affected nationwide was not disclosed.

Information Source:
Dataloss DB

records from this breach used in our total: 49

| November 7, 2006 | **Lehman College**
Bronx, New York | EDU | DISC | 768 |

A class of 2006 Fall graduation list was found to be accessible online. The file had only been available for 17 hours. Classes, majors, names, Social Security numbers, addresses, home phone numbers and dates of birth were on the list.

Information Source:
Dataloss DB

records from this breach used in our total: 768

| November 3, 2006 | **University of Virginia (UVA)**
Charlottesville, Virginia | EDU | DISC | 632 students |

Due to a computer programming error, Student Financial Services sent e-mail messages to students containing 632 other students' Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 632

| October 29, 2006 | **New York University**
New York, New York | EDU | PORT | 30,000 |

Backup CDs from the Continuing Medical Education program at NYU Medical Center were lost or stolen. Names, Social Security numbers, addresses, telephone and fax numbers, student ID numbers, debit or credit card information and degree information for students participating in the program between 1999 and the discovery of the loss may have been exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 30,000

October 19, 2006	**University of Minnesota** **Minneapolis-St.Paul, Minnesota**	EDU	PORT	200 students (not included in total)

In June, a University of Minnesota art department laptop computer stolen from a faculty member while traveling in Spain holds personally identifiable information of 200 students.

Information Source:
Media

records from this breach used in our total: 200

October 16, 2006	**Germanton Elementary School** **Germanton, North Carolina**	EDU	STAT	Unknown

A computer stolen from Germanton Elementary school holds students' SSNs. The data on the computer are encrypted.

Information Source:
Dataloss DB

records from this breach used in our total: 0

October 12, 2006	**University of Texas, Arlington** **Arlington, Texas**	EDU	STAT	2,500 students

http://www.uta.edu/oit/iso/Datatheft.php (http://www.uta.edu/oit/iso/Datatheft.php)

Two computers stolen from a University of Texas faculty member's home hold the names, SSNs, grades, e-mail addresses and other information belonging to approximately 2,500 students enrolled in computer science and engineering classes between fall 2000 and fall 2006. The theft occurred on September 29 and was reported on October 2.

Information Source:
Dataloss DB

records from this breach used in our total: 2,500

October 9, 2006	**Troy Athens High School** **Troy, Michigan**	EDU	PORT	4,400

For questions or comments, call (248) 823-4035

A hard drive stolen from Troy Athens High School in August contained transcripts, test scores, addresses and SSNs of students from the graduating classes of 1994 to 2004. The school district and the superintendent have notified all affected alumni by regular mail.

Information Source:
Dataloss DB

records from this breach used in our total: 4,400

October 5, 2006	**San Juan Capistrano Unified School District (CA)** **San Juan Capistrano, California**	EDU	STAT	Unknown

Five computers stolen from the HQ of San Juan Capistrano Unified School District likely contain the names, SSNs and dates of birth of district employees enrolled in an insurance program.

Information Source:
Dataloss DB

records from this breach used in our total: 0

October 3, 2006	**Willamette Educational Service District (ESD)** **Salem, Oregon**	EDU	STAT	4,500 Oregon high school students [not included in total because not thought to contain sensitive info. such as SSNs]

Seven computers stolen from a Willamette Educational Service District office were believed to contain personal information of 4,500 Oregon high school students. Backup tapes indicate the computers hold information about the students' school clubs but do not contain sensitive information.

Information Source:
Media

records from this breach used in our total: 0

September 29, 2006	**University of Iowa Department of Psychology** **Iowa City, Iowa**	EDU	HACK	14,500

A computer containing SSNs of 14,500 psychology department research study subjects was the object of an automated attack designed to store pirated video files for subsequent distribution.

Information Source:
Dataloss DB

records from this breach used in our total: 14,500

September 22, 2006	**Purdue University College of Science** **West Lafayette, Indiana**	EDU	STAT	2,482

 (866) 307-8520

A file in a desktop computer in the Chemistry Department may have been accessed illegitimately. The file contained names, SSNs, school, major, and e-mail addresses of people who were students in 2000.

Information Source:
Dataloss DB

records from this breach used in our total: 2,482

September 22, 2006	**University of Colorado, Boulder, Leeds School of Business** **Boulder, Colorado**	EDU	STAT	1,372 students and former students

(303) 492-8741

Two computers had been placed in storage during the school's move to temporary quarters in May. When they were to be retrieved Aug. 28, they were found missing. They had been used by 2 faculty members and included students' names, SSNs, and grades.

UPDATE (9/25/06): One of the computers was found.

Information Source:

records from this breach used in our total: 1,372

Dataloss DB

| September 20, 2006 | **Berry College via consultant Financial Aid Services Inc.** **Mount Berry, Georgia** | EDU | PHYS | 2,093 students and potential students (of those, 1,322 are currently enrolled) |

(800) 961-4692, [http://www.berry.edu/stulife/idprotect/ (http://www.berry.edu/stulife/idprotect/)](http://www.berry.edu/stulife/idprotect/)

Student applications for need-based financial aid were misplaced by a consultant -- in both paper and digital form. Data included name, SSN, and reported family income for students and potential students for the 2005-06 academic year.

Information Source: Dataloss DB

records from this breach used in our total: 2,093

| September 15, 2006 | **University of Texas San Antonio** **San Antonio, Texas** | EDU | HACK | 64,000 |

A hacker may have gained access to student and staff names, addresses and Social Security numbers. Students who received financial aid or worked at the University were affected. The breach was discovered during a routine risk assessment of the University's computer servers.

Information Source: Dataloss DB

records from this breach used in our total: 64,000

| September 15, 2006 | **Columbia University** **New York, New York** | EDU | INSD | 1,132 |

A temporary employee accessed the personal information of some University employees and used it to establish at least one fraudulent account. The former temp had access to the names, Social Security numbers, addresses, telephone numbers and direct deposit bank account information of a group of employees. The University discovered the breach on August 15 and began notifying affected individuals on August 18.

Information Source: Dataloss DB

records from this breach used in our total: 1,132

| September 8, 2006 | **University of Minnesota** **Minneapolis, Minnesota** | EDU | STAT | 13,084 students including SSNs of 603 students |

On August 14-15 eve, two computers were stolen from the desk of an Institute of Technology employee, containing information on students who were freshmen from 1992-2006 -- including names, birthdates, addresses, phone numbers, high schools attended, student ID numbers, grades, test scores, and, academic probation. SSNs of 603 students were also exposed.

Information Source: Dataloss DB

records from this breach used in our total: 603

| September 1, 2006 | **Virginia Commonwealth University (VCU)** **Richmond, Virginia** | EDU | DISC | 2,100 current and former |

students

http://old.ts.vcu.edu/security/id_exposure.html (http://old.ts.vcu.edu/security/id_exposure.html)

Personal information of freshmen and graduate engineering students from 1998 through 2005 was exposed on the Internet for 8 months (Jan. - Aug.) due to human error. It was discovered by a student who used a search engine to find her name. The data included SSNs and e-mail addresses.

Information Source:
Dataloss DB

records from this breach used in our total: 2,100

| August 26, 2006 | **University of South Carolina**
 Columbia, South Carolina | EDU | HACK | 6,000 |

TheState.com reported that the University of South Carolina warned 6,000 current and former students that their information, including Social Security numbers and birth dates, may have been breached when a server was accessed from outside the system.

Information Source:
Media

records from this breach used in our total: 6,000

| August 22, 2006 | **Beaverton School District**
 Beaverton, Oregon | EDU | PHYS | 1,600 employees |

Time slips revealing personal information were missing and presumed stolen following a July 24 break-in at a storage shed on the administration office's property. The time slips included names and SSNs but not addresses.

Information Source:
Dataloss DB

records from this breach used in our total: 1,600

| August 15, 2006 | **University of Kentucky**
 Lexington, Kentucky | EDU | DISC | 630 |

The names and SSNs of 630 students were posted on the University's financial aid web site between Friday and Monday, Aug. 11-14.

Information Source:
Dataloss DB

records from this breach used in our total: 630

| August 15, 2006 | **University of Kentucky Department of Georgraphy**
 Lexington, Kentucky | EDU | DISC | 80 |

About 80 geography students were notified Aug. 14 that their SSNs were inadvertently listed on an e-mail communication they all received telling them who their academic advisor would be for the coming year.

Information Source:
Dataloss DB

records from this breach used in our total: 80

| August 9, 2006 | **Hunter College of the City University of New York**
 New York, New York | EDU | STAT | Unknown |

A computer was stolen from the Writing Center in Thomas Hunter Hall on or around July 5. Its hard drive had a file that contained a list of student names and Social Security numbers. Students who participated in the Spring 2006 CPE intervention session were affected.

Information

Source:
Dataloss DB

records from this breach used in our total: 0

| August 1, 2006 | **Wichita State University**
Wichita, Kansas | EDU | HACK | 2,000 |

WSU learned on June 29 that someone gained unauthorized access into 3 computers in its College of Fine Arts box office, containing credit card information for about 2,000 patrons.

Information Source:
Dataloss DB

records from this breach used in our total: 2,000

| August 1, 2006 | **Wichita State University**
Wichita, Kansas | EDU | HACK | 40 (not included in total below because it is not known if SSNs were included in breached data) |

An intrusion into a WSU Psychology Department's server was discovered July 16. It contained information on about 40 applicants to the doctoral program.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| July 25, 2006 | **Belhaven College**
Jackson, Michigan | EDU | PORT | 300 |

An employee carrying a laptop was robbed at gunpoint on July 19 while walking to his car. The computer contained the names and SSNs of college employees.

Information Source:
Dataloss DB

records from this breach used in our total: 300

| July 16, 2006 | **Columbia University**
New York, New York | EDU | STAT | 78 |

On or around July 7, a computer was stolen from campus. The hard drive contained names, Social Security numbers, passport/visa numbers, tax identification numbers, home and business addresses, telephone contacts and email contacts.

Information Source:
Dataloss DB

records from this breach used in our total: 78

| July 14, 2006 | **Northwestern University**
Evanston, Illinois | EDU | HACK | 17,000 |

(888) 209-0097. http://www.northwestern.edu/newscenter/stories/2006/07/data.html (http://www.northwestern.edu/newscenter/stories/2006/07/data.html)

Files containing names and some personal information including SSNs were on 9 desktop computers that had been accessed by unauthorized persons outside the University. The computers were in the Office of Admissions and Financial Aid.

Information Source:
Dataloss DB

records from this breach used in our total: 17,000

July 14, 2006

**University of Iowa
Davenport, Iowa**

EDU   PORT   280

Laptop computer containing personal information of current and former MBA students was stolen. Data files included SSNs and some contact info.

Information Source:
Dataloss DB

records from this breach used in our total: 280

July 14, 2006

**California Polytechnic State University (Cal Poly)
San Luis Obispo, California**

EDU   PORT   3,020 students

Call (805) 756-2226 or (805) 756-2171

Laptop computer was stolen from the home of a physics department professor July 3. It included names and SSNs of physics and astronomy students from 1994-2004.

Information Source:
Security Breach Letter

records from this breach used in our total: 3,020

July 13, 2006

**Moraine Park Technical College
Beaver Dam, Wisconsin**

EDU   PORT   1,500

Additional locations: Fond du Lac and West Bend, WI

Computer disk (CD) with personal information of 1,500 students was reported missing. Information includes names, addresses, phone numbers & SSNs of apprenticeship students back to 1993.

Information Source:
Dataloss DB

records from this breach used in our total: 1,500

July 7, 2006

**University of Tennessee
Knoxville, Tennessee**

EDU   HACK   36,000

(866) 748-1680, http://security.tennessee.edu (http://security.tennessee.edu) . Additional locations: Chattanooga, Martin, Tullahoma and Memphis, TN

Hacker broke into a UT computer containing names, addresses and SSNs of about 36,000 past and current employees. The intruder used the computer from Aug. '05 to May '06 to store and transmit movies.

Information Source:
Dataloss DB

records from this breach used in our total: 36,000

July 5, 2006

**Columbia University
New York, New York**

EDU   DISC   98

An emergency contact list from the Columbia University School of International and Public Affairs was posted on an unsecure website on August 2005. Names, business and home phone numbers, addresses, emergency contact person and Social Security numbers were available.

Information Source: Dataloss DB

records from this breach used in our total: 98

| June 27, 2006 | **Empire Beauty School Inc.** **Brooklyn, New York** | EDU | PHYS | 1,132 |

The June 20 theft of a briefcase from an administrative employee's vehicle caused reports with the names and Social Security numbers of former students to be lost. A laptop was also stolen during the burglary, but it is unlikely that it had personal information.

Information Source: Dataloss DB

records from this breach used in our total: 1,132

| June 27, 2006 | **University of Rochester** **Rochester, New York** | EDU | DISC | 286 |

Former students' names and Social Security numbers were accidentally placed on a publicly accessible web page. Names, Social Security numbers and some standardized test scores were posted. The information was removed after the discovery and it appears that the information on the web page was accessed only once, on June 12 2006.

Information Source: Dataloss DB

records from this breach used in our total: 286

| June 24, 2006 | **Catawba County Schools** **Newton, North Carolina** | EDU | UNKN | 619 |

On June 22, it was discovered that a web site posted names, Social Security numbers, and test scores of students who had taken a keyboarding and computer applications placement test during the 2001-02 school year.

UPDATE:The web site containing the data has been removed.

Information Source: Dataloss DB

records from this breach used in our total: 619

| June 23, 2006 | **San Francisco State University** **San Francisco, California** | EDU | PORT | 3,000 |

www.sfsu.edu/%7Eadmisrec/reg/idtheft.html (http://www.sfsu.edu/%7Eadmisrec/reg/idtheft.html)

A faculty member's laptop was stolen from a car on June 1 that contained personal information of former and current students including Social Security numbers, and names and ins some instance, phone numbers and grade point averages.

Information Source: Dataloss DB

records from this breach used in our total: 3,000

| June 22, 2006 | **Ohio University** **Athens, Ohio** | EDU | HACK | 2,480 |

http://www.ohio.edu/datasecurity (http://www.ohio.edu/datasecurity)

A breach was discovered on a computer that housed IRS 1099 forms for vendors and independent contractors for calendar years 2004 and 2005.

Information Source:

records from this breach used in our total: 2,480

Media

| June 22, 2006 | **University of Kentucky** **Lexington, Kentucky** | EDU | PORT | 6,500 |

The personal data of current and former students including classroom rosters names, grades and Social Security numbers was reported stolen on May 26 following the theft of a professor's flash drive.

Information Source:
Dataloss DB

records from this breach used in our total: 6,500

| June 22, 2006 | **Ohio University** **Athens, Ohio** | EDU | HACK | Unknown |

http://www.ohio.edu/datasecurity/ (http://www.ohio.edu/datasecurity/)

A computer was compromised that hosted a variety of Web-based forms, including some that processed online business transactions. Although this computer was not set up to store personal information, investigators did discover files that contained fragments of personal information, including Social Security numbers. The data is fragmentary and it is not certain if the compromised information can be traced to individuals. Also found on the computer were 12 credit card numbers that were used for event registration.

Information Source:
Media

records from this breach used in our total: 0

| June 21, 2006 | **Lancaster General Hospital** **Lancaster, Pennsylvania** | EDU | STAT | Hundreds (at least 200) |

Date of letter sent to doctors: June 21, 2006 Date of news story: July 28, 2006

A desktop computer with personal information of hundreds of doctors was stolen from a locked office June 10. The unencrypted data included names, practice addresses, and SSNS of physicians on medical and dental staff.

Information Source:
Security Breach Letter

records from this breach used in our total: 200

| June 20, 2006 | **University of Alabama** **Birmingham, Alabama** | EDU | STAT | 9,800 |

In February a computer was stolen from a locked office of the kidney transplant program at the University of Alabama at Birmingham that contained confidential information of donors, organ recipients and potential recipients including names, Social Security numbers and medical information.

Information Source:
Dataloss DB

records from this breach used in our total: 9,800

| June 18, 2006 | **Ulster County Community College** **Stone Ridge, New York** | EDU | PORT | 18 |

A laptop that contained student information was stolen from a professor's office on or around June 28. The information included names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 18

June 17, 2006	**Western Illinios University** **Macomb, Illinois**	EDU	HACK	180,000

http://www.wiu.edu/securityalert/ (http://www.wiu.edu/securityalert/)

On June 5th, a hacker compromised a University server that contained names, addresses, credit card numbers and Social Security numbers of people connected to the University.

UPDATE (7/5/06): Number affected reduced from 240,000.

Information Source:
Dataloss DB

records from this breach used in our total: 180,000

June 12, 2006	**Barnard College** **New York, New York**	EDU	HACK	2,250

A hacking incident that was discovered on June 6 may have left the names and Social Security numbers of students and employees exposed. The computer that was compromised may have allowed the hacker to access information for all students and employees.

Information Source:
Dataloss DB

records from this breach used in our total: 2,250

June 11, 2006	**Adams State College** **Alamosa, Colorado**	EDU	PORT	184 Upward Bound students

A laptop computer stolen from a locked closet at Adams State College contained personally identifiable data belonging to 184 high school students who participated in the college's Upward Bound program over the last four years. The theft occurred on August 14, but it was not until late September that staff realized the computer held students' data.

Information Source:
Dataloss DB

records from this breach used in our total: 184

June 6, 2006	**University of Texas at El Paso** **El Paso, Texas**	EDU	HACK	4,719

Students demonstrated that student body and faculty elections could be rigged by hacking into student information including Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 4,719

June 6, 2006	**Empire State College** **Saratoga Springs, New York**	EDU	INSD	16

On December 15 of 2005, an intruder installed key-logger was discovered on a computer that had been used to access Social Security numbers. The keystroke capture program was installed by a relative of an employee in order to capture and read email messages that the staff member was sending. The program was in operation from March 2004 to January 2005 and again from October 2005 to December 15. The affected PC was removed from the office and had its hard drive scanned and cleaned.

Information Source:
Dataloss DB

records from this breach used in our total: 16

| June 1, 2006 | **Miami University**
Oxford, Ohio | EDU | PORT | 851 |

An employee lost a hand-held personal computer containing personal information of students who were enrolled between July 2001 and May 2006.

Information Source:
Dataloss DB

records from this breach used in our total: 851

| June 1, 2006 | **University of Kentucky**
Lexington, Kentucky | EDU | DISC | 1,300 |

Personal information of current and former University of Kentucky employees including Social Security numbers was inadvertently accessible online for 19 days in May.

Information Source:
Dataloss DB

records from this breach used in our total: 1,300

| May 30, 2006 | **Florida International University**
Miami, Florida | EDU | HACK | Unknown |

Hacker accessed a database that contained personal information on thousands of individuals, such as student and applicant names and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 26, 2006 | **California State University Stanislaus**
Turlock, California | EDU | DISC | 1,294 |

The University was informed that a file containing sensitive information remained in the Google cache and could be accessed by those with technological expertise. The file was first indexed in October of 2005. The file was deleted form the server, but it remained in the Google files cache. The file included names, addresses, Social Security numbers, and dates of birth of some current and former employees and their dependents.

Information Source:
Dataloss DB

records from this breach used in our total: 1,294

| May 24, 2006 | **Sacred Heart University**
Fairfield, Connecticut | EDU | HACK | Unknown |

It was discovered on May 8th that a computer containing personal information including names, addresses and Social Security numbers was breached. The University did not immediately release information on who the breach affected.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| May 23, 2006 | **University of Delaware**
Newark, Delaware | EDU | HACK | 1,076 |

A security breach of a Department of Public Safety computer server potentially exposed names, Social Security numbers and driver's license numbers. Individuals whose personal information was compromised were contacted.

Information Source:

records from this breach used in our total: 1,076

Dataloss DB

| May 16, 2006 | **University of California Berkeley**
Berkeley, California | EDU | HACK | 1,200 |

During an investigation of a computer virus, it was discovered that computers within an office may have been accessed without authorization from within the campus network. Student, faculty and staff names and Social Security numbers were on archived spreadsheets. The spreadsheets contained the personal information of people who requested campus cards between 1998 and 2004.

Information Source:
Dataloss DB

records from this breach used in our total: 1,200

| May 2, 2006 | **Ohio University Innovation Center**
Athens, Ohio | EDU | HACK | 35 |

http://www.ohio.edu/datasecurity (http://www.ohio.edu/datasecurity)

A server containing data including e-mails, patent and intellectual property files, and 35 Social Security numbers associated with parking passes was compromised.

Information Source:
Dataloss DB

records from this breach used in our total: 35

| May 2, 2006 | **Ohio University**
Athens, Ohio | EDU | HACK | 300,000
(137,000 SSNs) |

http://www.ohio.edu/datasecurity/ (http://www.ohio.edu/datasecurity/)

Hackers accessed a computer system of the school's alumni relations department that included biographical information and 137,000 Social Security numbers of alum.

UPDATE (8/30/07) : An Ohio judge has granted a motion to dismiss a case against Ohio University (OU) regarding security breaches of the school's computer systems that compromised alumni data. The two alumni who filed the lawsuit wanted OU to pay for credit monitoring services for everyone whose data were compromised. The judge said the pair had not proven that they had suffered damages for which they could be compensated.

Information Source:
Dataloss DB

records from this breach used in our total: 137,000

| April 26, 2006 | **Purdue University**
West Lafayette, Indiana | EDU | HACK | 1,351 |

A hacker accessed personal information including Social Security numbers of current and former graduate students, applicants to graduate school, and a small number of applicants for undergraduate scholarships. The information compromised goes back three years prior to the incident. Those who were affected were contacted.

Information Source:
Dataloss DB

records from this breach used in our total: 1,351

| April 24, 2006 | **University of Virginia**
Charlottesville, Virginia | EDU | STAT | Unknown |

A stolen computer contained the information of students who took engineering classes. The information included names, grades and student identification numbers. Hundreds of students are at risk of identity theft since Social Security numbers were used as student

identification numbers.

*Information
Source*:
Dataloss DB   *records from this breach used in our total: 0*

| April 24, 2006 | **College of New Paltz**
New Paltz, New York | EDU | HACK | Unknown |

A hacker accessed the Campus' primary web server and set up a file sharing system. The server involved also contained access databases
that had names and Social Security numbers.

*Information
Source*:
Dataloss DB   *records from this breach used in our total: 0*

| April 23, 2006 | **University of Texas McCombs School of Business**
Austin, Texas | EDU | HACK | 197,000 |

Foreign hackers accessed records containing names, biographical information and, in some cases, Social Security numbers and dates of
birth of current and prospective students, alumni, faculty members, corporate recruiters and staff members.

*Information
Source*:
Dataloss DB   *records from this breach used in our total: 197,000*

| April 21, 2006 | **University of Alaska, Fairbanks**
Fairbanks, Alaska | EDU | HACK | 38,941 |

A hacker had access to names, Social Security numbers, and partial e-mail addresses of current and former students, faculty, and staff.
The University reported that it would not contact those affected after a first and second notification. Anyone claiming to be from the
University after these notifications should be viewed with suspicion.

*Information
Source*:
Dataloss DB   *records from this breach used in our total: 38,941*

| April 14, 2006 | **University of South Carolina**
Columbia, South Carolina | EDU | DISC | 1,400 |

A department chair distributing information about summer courses sent an email containing sensitive information. A database containing
Social Security numbers of students was mistakenly added as an attachment and e-mailed to classmates.

*Information
Source*:
Dataloss DB   *records from this breach used in our total: 1,400*

| April 9, 2006 | **University of Medicine and Dentistry of New Jersey**
Newark, New Jersey | EDU | HACK | 1,850 |

Hackers accessed Social Security numbers, loan information, and other confidential financial information of students and alumni.

*Information
Source*:
Dataloss DB   *records from this breach used in our total: 1,850*

| April 1, 2006 | **Shorter College**
Rome, Georgia | EDU | HACK | Unknown |

A student was arrested for computer theft and hacking the College's computer network. The student may have accessed student, staff and faculty information.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| March 30, 2006 | **Connecticut Technical High School System**
Middletown, Connecticut | EDU | DISC | 1,250 |

Social Security numbers of faculty and administrators were mistakenly distributed via email to staff. The email went to 17 principals; at least one forwarded the email to her staff of 77. Those affected were contacted.

Information Source:
Dataloss DB

records from this breach used in our total: 1,250

| March 29, 2006 | **University of Nebraska Lincoln (UNL)**
Lincoln, Nebraska | EDU | DISC | 342 |

Students from the College of Engineering had Social Security numbers, email addresses, grade point averages and other personal information posted online. The information may have been posted since November of 2004 and was first noticed in summer of 2005. The problem was finally fixed during the week of March 29 when the file was removed from the Google server.

Information Source:
Dataloss DB

records from this breach used in our total: 342

| March 24, 2006 | **Vermont State Colleges**
Waterbury, Vermont | EDU | PORT | 14,000 |

Note: there are several locations in Vermont. We list the Office of the Chancellor as the primary location.

A laptop containing Social Security numbers and payroll data of students, faculty and staff associated with the five-college system was stolen. It contained information from as long ago as 2000.

Information Source:
Dataloss DB

records from this breach used in our total: 14,000

| March 24, 2006 | **California State University, Dominquez Hills**
Carson, California | EDU | PORT | 2,486 |

Students can leave a message at (310) 243-2305 for more information.

The theft of a laptop resulted in the exposure of student and potential student personal information. The University tightened access to campus servers and the campus network.

Information Source:
Dataloss DB

records from this breach used in our total: 2,486

| March 10, 2006 | **Long Island University, Alpha Chi National Honors Society**
Brooklyn, New York | EDU | DISC | 51 |

Students who applied to join Alpha Chi had their Social Security numbers and other personal information sent to an Honors student email list. The email was recalled immediately, but anyone who opened it right away would have been able to access the applicant information. The advisor responsible for the mistake asked the National Office to consider abandoning the use of Social Security numbers.

Information Source:

records from this breach used in our total: 51

Dataloss DB

| March 5, 2006 | **Georgetown University**
Washington, District Of Columbia | EDU | HACK | 41,000 |

A server was attacked that housed personal information including names, birthdates and Social Security numbers of District seniors served by the Office on Aging. Georgetown managed the server as part of a grant to manage information services provided by the D. C. Office of Aging.

Information Source:
Dataloss DB

records from this breach used in our total: 41,000

| March 3, 2006 | **Metropolitan State College of Denver (MSCD)**
Denver, Colorado | EDU | PORT | 93,000 |

http://www.mscd.edu/securityalert/ (http://www.mscd.edu/securityalert/)

A laptop containing student information was stolen. The information included names and Social Security numbers of students who registered for Metropolitan State courses between the 1996 fall semester and the 2005 summer semester.

Information Source:
Security Breach Letter

records from this breach used in our total: 93,000

| February 18, 2006 | **University of Northern Iowa**
Cedar Falls, Iowa | EDU | HACK | 6,000 |

A laptop computer holding W-2 forms of student employees and faculty was illegally accessed. The University warned students and faculty to monitor their bank accounts.

Information Source:
Dataloss DB

records from this breach used in our total: 6,000

| February 15, 2006 | **Old Dominion University**
Norfolk, Virginia | EDU | DISC | 601 |

An instructor posted a class roster containing names and Social Security numbers to a publicly accessible website. The information was posted during the spring semester of 2004. Letters were sent to affected students which contained websites where the students could check to see if they had been victims of identity theft.

Information Source:
Dataloss DB

records from this breach used in our total: 601

| February 1, 2006 | **University of Colorado, Colorado Springs (UCCS)**
Colorado Springs, Colorado | EDU | HACK | 2,500 |

Names, Social Security numbers, addresses and birth dates of current and former employees were accessed. A computer in the Personnel Department was hacked and infected with a virus. People employed by the University at anytime between the attack and 2004 are at risk. The virus infected other computers at the University and was part of a worldwide attack.

Information Source:
Dataloss DB

records from this breach used in our total: 2,500

| January 26, 2006 | **College of St. Scholastica**
Duluth, Minnesota | EDU | STAT | 12,000 |

A computer was stolen from a locked office in the College's information Technology Department on or around December 24. The computer had Social Security numbers and names of current and former students. The thief was caught and claims that none of the personal information was used.

Information Source:
Dataloss DB

records from this breach used in our total: 12,000

| January 25, 2006 | **University of Delaware**
Newark, Delaware | EDU | STAT | 159 |

Two separate breaches occurred on the campus during November and December. A computer from the School of Urban Affairs and Public policy was hacked and a back-up hard drive was stolen from the Department of Entomology and Wildlife Ecology. The hacking incident occurred between November 22 and 26 and exposed the Social Security numbers of 159 graduate students. The hard drive theft occurred between December 16 and 18 and the personal information of an unknown number of people was exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 159

| January 23, 2006 | **University of Notre Dame**
Notre Dame, Indiana | EDU | HACK | Unknown |

Hackers may have accessed Social Security numbers, credit card information and check images of people who donated to the University between November 22 of 2005 and January 12 of 2006.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| January 20, 2006 | **University of Kansas (Kansas University)**
Lawrence, Kansas | EDU | DISC | 9,200 |

A computer file with sensitive personal information was accessible to the public. Students who applied and paid an application fee online between April 29, 2001 and December 16, 2005 had their names, Social Security numbers, birth dates, addresses, phone numbers and credit card numbers exposed.

Information Source:
Dataloss DB

records from this breach used in our total: 9,200

| December 16, 2005 | **Colorado Technical University (CTU)**
Colorado Springs, Colorado | EDU | DISC | 300 |

An email was erroneously sent which contained names, phone numbers, email addresses, Social Security numbers and class schedules.

Information Source:
Security Breach Letter

records from this breach used in our total: 300

| December 12, 2005 | **Iowa State University**
Ames, Iowa | EDU | HACK | 5,500 |

At least one ISU computer was hacked. Social Security numbers and encrypted credit card numbers may have been obtained. Between 2,000 and 2,500 Social Security numbers are at risk and between 2,300 and 3,000 credit card numbers are at risk. Student, alumni, employee and volunteer information was put at risk.

Information

Source:
Dataloss DB

records from this breach used in our total: 5,500

| December 8, 2005 | **San Antonio Independent School District** **San Antonio, Texas** | EDU | PORT | 1,000 |

A laptop with personal information of more than a thousand teachers was stolen from an employee's unlocked car. The information included names, Social Security numbers and dates of birth.

Information Source:
Dataloss DB

records from this breach used in our total: 1,000

| December 8, 2005 | **J-Sargeant Reynolds Community College** **Richmond, Virginia** | EDU | DISC | 26,000 |

The names, Social Security numbers and addresses of students taking non-credit classes from 2000 to 2003 were posted online for months. The information was compiled for a mailing list, but an employee posted it on the College's server. A student informed officials of the mistake after accessing the information online. The College began the process of removing the information from the web.

Information Source:
Dataloss DB

records from this breach used in our total: 26,000

| December 7, 2005 | **Idaho State University, Office of Institutional Research** **Pocatello, Idaho** | EDU | HACK | Unknown |

Contact: Information Technology Services (208) 282-2872, http://www.isu.edu/announcement/ (http://www.isu.edu/announcement/)

ISU discovered a security breach in a server containing archival information about students, faculty, and staff, including names, Social Security numbers, birth dates, and grades. Anyone who was a student or employee between 1995 and 2005 could be affected.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| December 2, 2005 | **Cornell University** **Ithaca, New York** | EDU | HACK | 900 |

The University discovered a security breach last summer that exposed names, addresses, Social Security numbers, bank names and account numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 900

| December 1, 2005 | **University of San Diego** **San Diego, California** | EDU | HACK | 7,800 |

Hackers gained access to computers containing personal income tax data, including Social Security numbers, names, and addresses. Faculty members, students and vendors had their information compromised and were notified by the University.

Information Source:
Dataloss DB

records from this breach used in our total: 7,800

| November 23, 2005 | **University of Delaware** **Newark, Delaware** | EDU | HACK | 952 |

Two separate departments were breached by hacking within a short period of time. A School of Education computer with the names and Social Security numbers of 772 students registered in online education courses was attacked in late August. A Department of English computer that had the Social Security numbers of 180 faculty, graduate assistant and other teaching staff from the department was also hacked in August. The larger breach appears to be the result of someone attempting to establish an illegal movie sharing system. The smaller breach was a possible attempt to log onto and control one server in order to gain control over servers of other campuses. Those affected received notification and Social Security numbers have been removed from both servers.

Information Source:
Dataloss DB

records from this breach used in our total: 952

| November 18, 2005 | **Indiana University Kelley School of Business** **Indianapolis, Indiana** | EDU | HACK | 5,278 (4,778 SSNs reported) |

Students at the Indianapolis and Bloomington campuses may have been affected.

A hacker may have accessed the names, Social Security numbers and grades of students who enrolled in Introduction to Business courses between 2001 and 2005. The computer may have been hacked and installed with malware as early as August. A representative believes the breach occurred because the files were stored on a computer that did not have current anti-virus and system-protection software.

Information Source:
Dataloss DB

records from this breach used in our total: 4,778

| November 11, 2005 | **Georgia Tech University Office of Enrollment Services** **Atlanta, Georgia** | EDU | STAT | 13,000 |

On October 16 of 2005 computers were stolen from campus which contained the names, Social Security numbers, addresses and birth dates of current and prospective students. Notifications were sent to those who were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 13,000

| November 4, 2005 | **Keck School of Medicine, University of Southern California (USC)** **Los Angeles, California** | EDU | STAT | 50,000 |

A computer server containing names and Social Security numbers of patients, donors and employees was stolen from a campus computer room.

Information Source:
Security Breach Letter

records from this breach used in our total: 50,000

| October 29, 2005 | **University of Tennessee** **Knoxville, Tennessee** | EDU | DISC | 1,900 |

People at any of the University of Tennessee campuses may have been affected.

Nineteen hundred students and employees had their names and Social Security numbers posted on the Internet from spring of 2004 until the discovery in October of 2005. A student searched her name and found it listed with her Social Security number on a UT email discussion group site. Information pertaining to individuals who had either paid or owed small amounts of money to the University was shared among 10 employees and the information technology office. The information was mistakenly coded as public rather than private.

Information Source:
Dataloss DB

records from this breach used in our total: 1,900

| October 20, 2005 | **Monmouth University**
West Long Branch, New Jersey | EDU | DISC | 677 |

The names and Social Security numbers of 677 students were posted online for over four months. The University corrected the error and notified students after a student notified them of the problem. A glitch seems to have caused the information to be found through a simple Internet search.

Information Source:
Dataloss DB

records from this breach used in our total: 677

| October 20, 2005 | **Vermont Technical College**
Randolph Center, Vermont | EDU | DISC | Unknown |

Names, Social Security numbers, addresses, SAT scores and ethnicity of all students enrolled during 2003 were posted online from January 2004 until the mistake was discovered in October of 2005. Someone accidentally sent the data to a publicly accessible place.

Information Source:
Dataloss DB

records from this breach used in our total: 0

| October 15, 2005 | **Montclair State University**
Montclair, New Jersey | EDU | DISC | 9,100 |

Names and Social Security numbers of undergraduates were posted online for nearly four months. An undergraduate alerted the University after running a Google.com search of his name. The University warned all students of the problem.

Information Source:
Dataloss DB

records from this breach used in our total: 9,100

| September 29, 2005 | **University of Georgia**
Athens, Georgia | EDU | HACK | 1,600 |

A hacker may have accessed the names and Social Security numbers of at least 1,600 people working for the College of Agricultural and Environmental Sciences. The University is attempting to contact individuals who may have been affected.

Information Source:
Dataloss DB

records from this breach used in our total: 1,600

| September 22, 2005 | **City University of New York**
New York, New York | EDU | DISC | 771 |

An unprotected payroll link exposed personal information for Hunter College Campus Schools. Those affected included 335 Queens College law school students, 265 current workers and 171 former workers at local elementary and high schools. All affected people were contacted.

Information Source:
Dataloss DB

records from this breach used in our total: 771

| September 15, 2005 | **Miami University**
Hamilton, Ohio | EDU | DISC | 21,762 |

A report containing Social Security numbers and grades of students was accessible online for three years. The University is attempting to contact those affected via letters and emails. A graduate alerted the University to the exposure after running a Google.com search of her name.

Information

Source:
Dataloss DB

records from this breach used in our total: 21,762

September 10, 2005 | **Kent State University**
Kent, Ohio

EDU   STAT   100,000

Five desktop computers were stolen from the locked offices of two deans. Names, Social Security numbers, and grades were on the computers. The information goes back to 2000 for students and 2002 for instructors. Affected students and professors were alerted by the University.

Information Source:
Dataloss DB

records from this breach used in our total: 100,000

August 30, 2005 | **California State University, Chancellor's Office**
Long Beach, California

EDU   HACK   154

A computer virus attack exposed names and Social Security numbers. Those affected included two financial aid administrators and 152 students enrolled at various Cal State Universities. Those affected were contacted.

Information Source:
Dataloss DB

records from this breach used in our total: 154

August 30, 2005 | **Stark State College of Technology**
North Canton, Ohio

EDU   DISC   7,058

Students attempting to access their grades, financial aid information and academic standing were able to view the information of other students. Social Security numbers, GPA, and course enrollment were viewable. A glitch is believed to be the source of the problem.

Information Source:
Dataloss DB

records from this breach used in our total: 7,058

August 27, 2005 | **University of Florida, Health Sciences Center, ChartOne**
Gainesville, Florida

EDU   PORT   3,851

A contractor's laptop containing patient names, Social Security numbers, dates of birth, and medical record numbers was stolen. A letter was sent to the affected patients.

Information Source:
Dataloss DB

records from this breach used in our total: 3,851

August 19, 2005 | **University of Colorado**
Denver, Colorado

EDU   HACK   49,000

A hacker may have gained access to personal information from June of 1999 to May of 2001, and fall of 2003 to summer of 2005. The information included current and former student names, Social Security numbers, addresses and phone numbers. The University contacted individuals who were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 49,000

August 17, 2005 | **California State University, Stanislaus**
Turlock, California

EDU   HACK   900

The names and Social Security numbers of student workers were exposed during a hacker attack. The student workers were contacted by the University.

Information Source:
Dataloss DB

records from this breach used in our total: 900

| August 10, 2005 | **University of North Texas**
Denton, Texas | EDU | HACK | 39,000 |

A server containing housing records, financial aid inquiries, and in some cases credit card numbers was hacked. UNT sent letters to current, former, and prospective students whose information may have been accessed.

Information Source:
Dataloss DB

records from this breach used in our total: 39,000

| August 9, 2005 | **Sonoma State University**
Rohnert Park, California | EDU | HACK | 61,709 |

Hackers broke into a computer system and may have accessed the names and Social Security numbers of people who applied, attended, or worked at the University between 1995 and 2002. University officials attempted to notify those who were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 61,709

| August 9, 2005 | **University of Utah**
Salt Lake City, Utah | EDU | HACK | 100,000 |

A server containing library archival databases was hacked. The server included names and Social Security numbers of former University employees. The University issued a warning that people may try to get personal information by posing as University officials involved in the investigation.

Information Source:
Dataloss DB

records from this breach used in our total: 100,000

| August 5, 2005 | **Madison Area Technical College**
Madison, Wisconsin | EDU | PHYS | 100 |

A news crew found around 100 applications in a MATC dumpster. The applications showed names, contact information, Social Security numbers, birth dates, academic records and canceled checks. The applications and transcripts go back to at least 2002. The College agreed to lock the dumpster and destroy documents in a trash compactor on a more frequent basis. It did not state that it would begin shredding documents before dumping them.

Information Source:
Dataloss DB

records from this breach used in our total: 100

| August 4, 2005 | **Anderson College**
Anderson, North Carolina | EDU | PHYS | 800 |

A bag with student resident hall assignments was found on campus. The paperwork also had the students' Social Security numbers. The documents were destroyed and a new program that will prevent unauthorized faculty and staff from accessing student Social Security numbers was developed.

Information Source:
Dataloss DB

records from this breach used in our total: 800

| August 2, 2005 | **University of Colorado**
Denver, Colorado | EDU | HACK | 36,000 |

Hackers accessed files containing names, photographs, Social Security numbers, and University meal card information. Around 7,000 staff members, 29,000 current students, and some former students were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 36,000

| July 31, 2005 | **California State Polytechnic University (Cal PolyPomona)**
Pomona, California | EDU | HACK | 31,077 |

Hackers gained access to two computers containing names, Social Security numbers and transfer records. Applicants, current students, current and former faculty, and staff were affected.

Information Source:
Dataloss DB

records from this breach used in our total: 31,077

| July 30, 2005 | **California State University, Dominguez Hills**
Carson, California | EDU | HACK | 9,613 |

Hackers accessed several computers containing personal information such as names and Social Security numbers. The students who were affected were emailed.

Information Source:
Dataloss DB

records from this breach used in our total: 9,613

| July 30, 2005 | **Austin Peay State University**
Clarksville, Tennessee | EDU | DISC | 1,500 |

The University removed student Social Security numbers, grade point averages and names that were accidentally posted. A student alerted the University to the problem after searching his name and finding the information on the website. A school employee put the internal documents on the website to email other staff members the information, but forgot to remove the information from the website.

Information Source:
Dataloss DB

records from this breach used in our total: 1,500

| July 21, 2005 | **University of Colorado, Boulder**
Boulder, Colorado | EDU | HACK | 49,000 |

Prospective students, current students, staff, faculty and University health care service recipients may have had their data exposed in a campus server breach. The information included names, Social Security numbers, addresses, student ID numbers, birth dates, and lab test information. The University mailed letters and sent emails to the individuals affected.

UPDATE (08/20/2005) The number of students affected was increased from an estimate of 42,000 to 49,000.

Information Source:
Dataloss DB

records from this breach used in our total: 49,000

| July 12, 2005 | **University of Southern California (USC)**
Los Angeles, California | EDU | DISC | 270,000 possibly accessed, dozens exposed |

A reporter contacted USC based on an individual's claim to be able to access personal information on college applicants online. USC removed the site pending investigation and sent letters to affected individuals.

Information Source:
Security Breach Letter

records from this breach used in our total: 270,000

| July 7, 2005 | **Michigan State University**
East Lansing, Michigan | EDU | HACK | 27,000 |

Student information was compromised during an attack on the College of Education server. The information included Social Security numbers, names, addresses, student courses, and personal identification numbers. The breach occurred in April and students were emailed in July.

Information Source:
Dataloss DB

records from this breach used in our total: 27,000

| July 1, 2005 | **University of California San Diego**
La Jolla, California | EDU | HACK | 3,300 |

A University server was hacked in April. The server contained Social Security numbers, driver's license numbers, and credit card numbers from people who attended or worked at UCSD Extension between the time of the incident and 2000. UCSD contacted those who were affected two months after the incident.

Information Source:
Dataloss DB

records from this breach used in our total: 3,300

| June 25, 2005 | **University of Connecticut (UCONN)**
Storrs, Connecticut | EDU | HACK | 72,000 |

University officials became aware of an October 26, 2003 hacking incident. The personal information included Social Security numbers and addresses for students, faculty, and staff. The University began contacting those affected in June of 2005.

Information Source:
Dataloss DB

records from this breach used in our total: 72,000

| June 18, 2005 | **University of Hawai'i**
Honolulu, Hawaii | EDU | INSD | 150,000 |

A former librarian with access to the personal information of students, faculty, staff and patrons was convicted of Social Security fraud. The former librarian used Social Security information to obtain fraudulent loans. The University used Social Security numbers to track who checked out library materials. At the time of the press release it was unclear whether any information had been stolen from the University.

Information Source:
Dataloss DB

records from this breach used in our total: 150,000

| June 17, 2005 | **Kent State University**
Kent, Ohio | EDU | PORT | 1,400 |

A laptop containing the names, Social Security numbers, and in some cases birthdays of current and former University employees was stolen from a human resources administrator's car.

Information

records from this breach used in our total: 1,400

June 4, 2005	**Duke University Medical Center** **Durham, North Carolina**	EDU	HACK	14,000 (No reports of full SSNs or financial information)

A hacker broke into the computer system, stealing thousands of passwords and fragments of Social Security numbers. Fourteen thousand affected people were notified, including 10,000 employees of Duke University Medical Center.

records from this breach used in our total: 0

May 27, 2005	**Cleveland State University** **Cleveland, Ohio**	EDU	PORT	44,420

A laptop containing personal information from applicants, current students, and former students was stolen from the University's admissions office. The information included Social Security numbers and addresses from as far back as 2001. Letters were sent to those affected.

UPDATE (12/24/05):CSU found the stolen laptop

records from this breach used in our total: 44,420

May 19, 2005	**Valdosta State University** **Valdosta, Georgia**	EDU	HACK	40,000

A computer server containing campus ID card information and Social Security numbers was hacked. The cards were designed to be used as debit cards by students and employees.

records from this breach used in our total: 40,000

May 18, 2005	**Jackson Community College** **Jackson, Michigan**	EDU	HACK	8,000

A hacker may have downloaded the passwords and Social Security numbers of employees and students. The College sent new, high security passwords to students and employees.

records from this breach used in our total: 8,000

May 18, 2005	**University of Iowa** **Iowa City, Iowa**	EDU	HACK	30,000

A computer containing credit card numbers and campus ID numbers for University Book Store customers was breached by a hacker.

records from this breach used in our total: 30,000

May 12, 2005	**Hinsdale Central High School** **Hinsdale, Illinois**	EDU	HACK	2,400

Two students were accused of hacking into the School's computer system and stealing student and staff Social Security numbers. The students had the information for months before being caught. Letters were sent to affected families. The Social Security Administration and the Federal Trade Commission were also notified.

Information Source: Dataloss DB

records from this breach used in our total: 2,400

May 11, 2005	**Stanford University** **Stanford, California**	EDU	HACK	9,900

The University's Career Development Center was hacked. This exposed the names, Social Security numbers, and other personal information of users. Names and credit card information for some employers that registered with the site were also in the database.

Information Source: Dataloss DB

records from this breach used in our total: 9,900

May 5, 2005	**Purdue University** **West Lafayette, Indiana**	EDU	HACK	11,360

Hackers accessed a program which contained University credit card information and the Social Security numbers of current and former employees. Letters were sent to employees and former employees.

Information Source: Dataloss DB

records from this breach used in our total: 11,360

April 29, 2005	**Oklahoma State University** **Stillwater, Oklahoma**	EDU	PORT	37,000

A laptop used for student job placement seminars was lost or stolen. It contained the Social Security numbers of current and former students.

Information Source: Dataloss DB

records from this breach used in our total: 37,000

April 28, 2005	**Georgia Southern University** **Statesboro, Georgia**	EDU	HACK	tens of thousands (at least 20,000)

Hackers accessed a University server which contained thousands of credit card and Social Security numbers collected over three years. Students who received bookstore credit through scholarship or financial aid between the fall 2003 and spring of 2005 semesters, and anyone who made credit purchases at campus stores, stadium, or website are at risk. Email alerts were sent to students and alumni.

Information Source: Dataloss DB

records from this breach used in our total: 20,000

April 26, 2005	**Michigan State University's Wharton Center** **East Lansing, Michigan**	EDU	HACK	40,000

A hacker may have stolen the credit card information of visitors attending a performing arts venue. Warnings were sent to Wharton visitors who used their credit cards anytime between September of 2003 and the incident.

Information Source: Dataloss DB

records from this breach used in our total: 40,000

| April 21, 2005 | **Carnegie Mellon University** **Pittsburgh, Pennsylvania** | EDU | HACK | 19,000 |

The compromised information included Social Security numbers and grades from master's alumni classes 1997 through 2004, job offer information from master's alumni classes 1985 through 2004, contact information for all alumni, and Social Security numbers and grades from doctoral students enrolled between 1998 and 2004. Between 5,000 and 6,000 of those affected had their credit card information and Social Security numbers compromised. Emails and letters were sent to those who were affected.

Information Source: Dataloss DB

records from this breach used in our total: 19,000

| April 11, 2005 | **Tufts University** **Boston, Massachusetts** | EDU | HACK | 106,000 |

RuffaloCODY is the software management company.

The University's donor database was breached sometime in late 2004. The database was managed by a software company for nonprofit organizations named RuffaloCODY. Letters were sent to the alumni who may have had their personal information stolen.

Information Source: Dataloss DB

records from this breach used in our total: 106,000

| April 6, 2005 | **University of California, San Francisco (UCSF)** **San Francisco, California** | EDU | HACK | 7,000 |

A server in the accounting and personnel departments was hacked. It contained information on 7,000 students, faculty, and staff members. The affected individuals were notified March 23.

Information Source: Dataloss DB

records from this breach used in our total: 7,000

| April 5, 2005 | **University of California, Davis** **Davis, California** | EDU | HACK | 1,100 |

The names and Social Security numbers of students, faculty, visiting speakers and staff may have been compromised when a hacker accessed a main computer.

Information Source: Dataloss DB

records from this breach used in our total: 1,100

| March 25, 2005 | **Purdue University** **West Lafayette, Indiana** | EDU | HACK | 1,200 (not included in total because news stories are not clear if SSNs or financial information were exposed) |

Computers in the College of Liberal Arts' Theater Dept. were hacked, exposing personal information of employees, students, graduates, and business affiliates.

Information Source:
Dataloss DB

records from this breach used in our total: 0

March 20, 2005 | **Northwestern University** | EDU | HACK | 17,500
Evanston, Illinois

Hackers gained access to multiple computers and gathered user ID and password information from the University's network. The personal information for around 500 faculty members, 2000 staff members, and 14,000 alumni was compromised.

Information Source:
Media

records from this breach used in our total: 17,500

March 20, 2005 | **University of Nevada, Las Vegas** | EDU | HACK | 5,000
Las Vegas, Nevada

A hacker was caught accessing the University's server and may have gotten information from the Student Exchange and Visitor Information System (SEVIS).

Information Source:
Dataloss DB

records from this breach used in our total: 5,000

March 16, 2005 | **California State University, Chico** | EDU | HACK | 59,000
Chico, California

A university housing and food service computer server containing names and Social Security numbers of faculty, staff, students, former students, and prospective students was hacked.

Information Source:
Dataloss DB

records from this breach used in our total: 59,000

March 11, 2005 | **University of California, Berkeley** | EDU | PORT | 98,400
Berkeley, California

A laptop containing the Social Security numbers of doctoral degree recipients from 1976 to 1999, graduate students enrolled between 1989 and 2003, and graduate school applicants between fall 2001 and spring of 2004 was stolen. Birth dates and addresses for about one-third of the affected people were also on the laptop.

Information Source:
Dataloss DB

records from this breach used in our total: 98,369

March 11, 2005 | **Boston College** | EDU | HACK | 120,000
Boston, Massachusetts

A hacker gained access to a phone banking database that included alumni addresses and Social Security numbers.

Information Source:
Dataloss DB

records from this breach used in our total: 120,000

January 22, 2005 | **University of Northern Colorado** | EDU | PORT | 15,790 (15,790 employees and an unknown
Greeley, Colorado

number of
employee
beneficiaries)

A hard drive was lost or stolen. It contained information on current and former University employees and their beneficiaries and dates back to April of 1997. Names, dates of birth, SSNs, addresses, bank account numbers and routing numbers may have been accessed.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 15,790

January 18, 2005 **University of California, San Diego**
                  San Diego, California

EDU   HACK   3,500

A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 3,500

January 10, 2005 **George Mason University**
                  Fairfax, Virginia

EDU   HACK   32,000

Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the University's main ID server.

*Information
Source*:
Dataloss DB

records from this breach used in our total: 32,000

Breach Total

607,255,163 RECORDS BREACHED
(Please see explanation (/data-breach-FAQ#2) about this total.)
from 3,658 DATA BREACHES made public since 2005