Published on *Privacy Rights Clearinghouse* (http://www.privacyrights.org)
Today's Date: Dec 06, 2013

Chronology of Data Breaches Custom Sort

Chronology of Data Breaches

Custom Sort
Select your desired results. Then click "Go!"
to generate a PDF which you can save or print.

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 [1]

Help Guide [2]

Return to Chronology main page. [3]

Breach Subtotal

Breaches currently displayed:
Breach Types: DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN
Organization Types: EDU
Years: 2013
2,878,317 Records in our database from.
43 Breaches made public fitting this criteria

Date Made Public	Name	Entity	Type	Total Records
December 3, 2013	**Chicago Public S hools Chicago, Illinois**	EDU	DISC	2,000 (No Social Security numbers or

Chicago, Illinois

financial information reported)

The vision exam dates, diagnoses, dates of birth, genders, identification numbers, and school names of students were accidentally made available to the public online between June 18 and July 31, 2013. The breach was discovered on October 7 and the Chicago vision examp program information was removed. The information was viewed by 14 people during that time. All cached and archived versions of the information were also removed from the Internet.

Information Source: Databreaches.net

records from this breach used in our total: 0

November 27, 2013 | **Maricopa County Community College District**
Phoenix, Arizona | EDU | UNKN | 2.49 million

An unspecified data breach may have exposed the information of current and former students, employees, and vendors. Names, Social Security numbers, bank account information, and dates of birth may have been viewed by unauthorized parties.

UPDATE (12/02/2013): Student academic information may have also been exposed. The Maricopa County Community College District's governing board will spend as much as $7 million to notify and offer credit monitoring to those who may have been affected.

Information Source: Media

records from this breach used in our total: 2,490,000

November 19, 2013 | **Sachem Central School District**
Lake Ronkonkoma, New York | EDU | HACK | 15,000

Sachem's notice can be found here:
[4] http://www.sachem.edu/home/pdf/QAData11192013.pdf [4]

Two breaches in the summer of 2013 and November of 2013 resulted in the exposure of student information. The sensitive information that was exposed in July may have been accidentally exposed through an administrative error.

A second breach was discovered on November 8 when the Superintendent learned that student information had been posted on a publicly accessible webpage. The investigation of the November breach is ongoing. Student names and ID numbers were the primary types of data that were exposed in both incidents.

UPDATE (11/23/2013): A student of Sachem North High School pleaded not guilty to computer trespass and was released without bail. The student may have also accessed information in 2012. A list of 15,000 students' information that dated back to the early 2000s was discovered online. A list of 130 students who received instructional services in an alternative setting in the 2010-2011 school year was also discovered online.

Information Source: Security Breach Letter

records from this breach used in our total: 0

November 15, 2013 | **Greencastle Community School Corporation**
Greencastle, Indiana | EDU | HACK | Unknown

Greencastle Community School Corporation notified parents of a security issue involving improprer access by students. Several students from Greencastle High School found a list of student network passwords and were able to access a limited amount of confidential student files on the school network. Students in grades three through 12 may have had breakfast or lunch expenses falsely charged to their names and students with unauthorized access may have been able to access the network under other students' accounts.

Information Source: Media

records from this breach used in our total: 0

November 7, 2013 | **Washington State University Pullman, Washington** | EDU | PORT | 300

The October 11 theft of two external hard drives may have exposed the information of students, current employees, and former employees. Administrative and financial information such as Social Security numbers may have been exposed.

Information Source: Media

records from this breach used in our total: 300

October 31, 2013 | **Milwaukee Public School District, Express Scripts Milwaukee, Wisconsin** | EDU | DISC | 6,000

Social Security numbers were printed on the outside of letters that were sent to a third party vendor. As many as 6,000 letters were sent to MPS Medicare D recipients.

Information Source: Media

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

October 25, 2013 | **Michigan State University East Lansing, Michigan** | EDU | HACK | Unknown

Michigan State University provided a notification here [5]: http://police.msu.edu/crimealert10202013.asp [5]

An unauthorized user was able to modify employee banking information. The breach was discovered on October 18 when two employees reported receiving email confirmations of changes to their direct-deposit designations. The unauthorized user may have obtained valid payroll credentials by using a phishing attack. The HR/Payroll systems were taken offline on Friday, October 18 and were expected to become active again on October 21.

Information Source: Media

records from this breach used in our total: 0

October 23, 2013 | **University of Southern Maine Portland, Maine** | EDU | PHYS | Unknown

Someone broke into a University van and stole campus keys. The keys could give them access to nearly 50 Portland and Gorham campus buildings. The University is in the process of replacing locks of the affected buildings. Student, personnel, and other records may be accessible. Faculty, staff, and students were notified of the incident and encouraged to shut electronic devices down when leaving them unattended. They were also advised to not leave sensitive information or belongings in campus buildings without additional locks.

Information Source: Media

records from this breach used in our total: 0

October 17, 2013 | **California State University Sacramento (Sacramento State University) Sacramento, California** | EDU | HACK | 1,800

In August, Sacramento State University was notified that a computer server had been hacked. It contained the Social Security numbers, driver's license numbers, and other personal information of staff members. The cause and extent of the breach were determined in late September and staff members were notified in mid-October.

Information Source: Media

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

October 17, 2013	**University of Arizona Tucson, Arizona**	EDU	HACK	9,080

A July 29 breach of the University of Arizona's College of Law website allowed intruders to access class rosters and applicant lists. University of Arizona law students and applicants may have had their names, Social Security numbers, usernames, and passwords exposed.

Information Source: Media

records from this breach used in our total: 9,080

October 9, 2013	**University of California San Francisco Medical Center (UCSF) San Francisco, California**	EDU	PORT	3,541 (Unknown number of Social Security numbers exposed)

A total of 3,541 patients were affected by the September 10 theft of an unencrypted laptop from an employee's vehicle. A subset of the 3,541 patients who were affected had their Social Security numbers exposed.

UPDATE (10/08/2013): Paper documents with patient names, Social Security numbers, dates of birth, and medical information were also stolen.

Information Source: Media

records from this breach used in our total: 0

October 1, 2013	**McHenry County College, Ellucian Crystal Lake, Illinois**	EDU	DISC	Unknown

McHenry County College's software vendor Ellucian accidentally sent the personal information of current and former McHenry County College students and staff to three other junior colleges. Social Security numbers and other information were sent to Morton, Prairie State, and Triton.

Information Source: Media

records from this breach used in our total: 0

September 28, 2013	**Virginia Polytechnic Institute and State University (Virginia Tech) Blacksburg, Virginia**	EDU	HACK	144,963 (No Social Security numbers or financial information reported)

The University's statement can be found here: http://www.vtnews.vt.edu/articles/2013/09/092413-hr-hrserver.html [6]

The computer server of Virginia Tech's Department of Human Resources was accessed on August 28. The information of people who applied online to Virginia Tech between 2003 and 2013 may have been accessed. No Social Security numbers or financial information was exposed. A total of 16,642 job applicants had their driver's license numbers exposed. The remaining job applicants had not submitted this information.

Information Source: Media

records from this breach used in our total: 0

September 23, 2013 | **Stanford University**
Stanford, California | EDU | HACK | Unknown

Stanford University ID holders (SUNet) users had their account passwords and other information exposed. The breach occurred sometime during the summer of 2013 and continued into the fall. The full extent of the breach was not revealed. SUNet users were instructured to change their passwords before accessing the system again.

Information Source: Media

records from this breach used in our total: 0

September 10, 2013 | **University of South Florida (USF) Health**
Tampa, Florida | EDU | INSD | 140

Police searched the car of a University custodial employee and found USF Physicians Group patient billing information. Names, Social Security numbers, and dates of birth had been exposed. The employee no longer works for the University and patients were sent a notification letter in late July.

Information Source: Media

records from this breach used in our total: 140

September 6, 2013 | **Conexis, State of Virginia**
Blacksburg, Virginia | EDU | DISC | 13,000

Employees of the state of Virginia who are enrolled in the Commonwealth's 2014 Flexible Spending Account had their information exposed. Conexis erroneously sent summary reports of Blue Cross/Blue Shield Flexible Spending Account Services to 11 state human resources and payroll employees. The reports included participants from across the state rather than from specific locations related to the human resources and payroll employees' work. The human resources and payroll employees who received information that was not intended for them signed a certification confirming that they had deleted or destroyed the information.

Information Source: Media

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

August 22, 2013 | **San Francisco State University - College of Extended Learning**
San Francisco, California | EDU | HACK | Unknown

A server that contained the personal information of students was breached on March 25, 2013. Federal law enforcement notified San Francisco State University of the breach on June 11. The College of Extended Learning notified students of the issue on August 12. An unspecified number of names, Social Security numbers, and other personal information was exposed.

Information Source: Media

records from this breach used in our total: 0

August 21, 2013	**Emory University** **Atlanta, Georgia**	EDU	HACK	Unknown

Anyone with an Emory University netID/username is being advised to change their account password due to a breach. Emory University stated that it appears the attack on their information technology infrastructure is similar to attacks that similar organizations have seen in the past few months. Emory University also stated that it does not appear that sensitive information was accessed.

Information Source: Media

records from this breach used in our total: 0

August 16, 2013	**Ferris State University** **Big Rapids, Michigan**	EDU	HACK	62,000 (39,000 Social Security numbers)

An unauthorized person gained access to the school's computer network. Campus ID numbers, names, and possibly other information of staff and students were exposed. In addition to the 39,000 people who had their files with Social Security numbers exposed, 19,000 more indidviduals were notified of the breach.

UPDATE (10/22/2013): It is estimated that 62,000 people were affected and $380,000 was spent investigating the breach. This number includes providing services to those who were affected.

Information Source: Media

records from this breach used in our total: 39,000

August 9, 2013	**Auburn University - School of Forestry and Wildlife Sciences** **Auburn, Alabama**	EDU	DISC	Unknown

Spreadsheets with donor and alumni information were accidentally uploaded to a publicly accessible server after an administrative error. The error was discovered on June 19 and Auburn's IT office removed the information. Names, Social Security numbers, maiden names, mailing addresses, first year at Auburn, graduation year, alumni status, email addresses, and phone numbers were exposed.

Information Source: Databreaches.net

records from this breach used in our total: 0

July 30, 2013	**University of Delaware** **Newark, Delaware**	EDU	HACK	74,000

Additional information can be found on the University of Delaware's website here [7]: http://www.udel.edu/it/response/

Students and staff members may have had their information exposed during a hacking incident. The hacker or hackers were able to exploit a vulnerability in software acquired by a vendor. Names, addresses, Social Security numbers, and university ID numbers were exposed.

UPDATE (08/19/2013): An additional 2,000 people were affected. They were not employees but had received payment from the University of Delaware.

Information Source: Media

records from this breach used in our total: 74,000

July 26, 2013	**Stanford University Stanford, California**	EDU	HACK	Unknown

People who used Stanford University's computer network have been asked to reset their passwords. Stanford released few details but stated that it does not appear that Social Security numbers and financilai nformation were accessed or exposed.

Information Source: Media

records from this breach used in our total: 0

July 19, 2013	**University of Virginia, Aetna Health Care Charlottesville, Virginia**	EDU	DISC	18,700

A mailing error by a third-party mailing vendor used by Aetna Health Care resulted in the Social Security numbers of students being exposed in open-enrollment brochures.

Information Source: Media

records from this breach used in our total: 18,700

July 11, 2013	**Guildford County Schools, Page High School Greensboro, North Carolina**	EDU	DISC	456 (No SSNs or financial information reported)

Parents with questions may call 336-332-0810.

A Guildford County Schools employee accidentally emailed a PDF file that contained Page High School student personal information. Student names, addresses, phone numbers, course enrollments, grades, school district identification numbers, and other transcript data were in the PDF file. The information was emailed to a single guardian on July 2, 2013.

Information Source: Media

records from this breach used in our total: 0

June 28, 2013	**University of South Carolina Columbia, South Carolina**	EDU	PORT	6,300

The April theft of a faculty laptop resulted in the exposure of current and former student information. The laptop was stolen from a locked room in the Department of Physics and Astronomy. It contained a file with the names, emails, and Social Security numbers of up to 6,300 University of South Carolina students who had taken one of four physics courses between January of 2010 and the fall 2012 semester.

Information Source: Media

records from this breach used in our total: 6,300

June 24, 2013	**Florida State University, Florida Department of Education Tallahassee, Florida**	EDU	DISC	47,000

The information of 47,000 Florida teachers was publicly accessible for 14 days after a data transfer at Florida State University. The information was from teachers participating in state prep programs. The Department of Education used Florida State University as the contractor for the transfer of teacher data.

UPDATE (06/26/2013): People who participated in Florida teacher preparation programs during the 2009 -2010 and 2011-2012 academic years were affected.

Information Source: Media

records from this breach used in our total: 47,000

June 5, 2013 **University of Massachusetts - Amherst**
Amherst, Massachusetts
EDU HACK 1,700

The information of almost 1,700 clients of the Center for Language, Speech, and Hearing may have been exposed. A computer workstation was found to be infected by a malicious software program. Client Social Security numbers, addresses, names of health insurers, and primary health care or referring doctors may have been accessible because the computer was compromised.

Information Source: Media

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

June 3, 2013 **Champlain College**
Burlington, Vermont
EDU PORT 14,217

Those with questions may call 877-643-2062.

During the weekend of June 3, a hard drive was discovered to have been misplaced. The device had been left unattended in a computer lab for about two days in March. The hard drive contained names, Social Security numbers, and other information related to admissions and financial aid for the Fall 2010 through the February 2013 school terms. Some graduate and continuing professional studies students may have also been affected.

Information Source: Media

records from this breach used in our total: 14,217

May 3, 2013 **Schoenbar Middle School**
Ketchikan, Alaska
EDU HACK Unknown

A ring of middle school students were able to gain access to and control of more than 300 computers by phishing for teacher administrative codes. At least 18 students were involved. The breach happened when students used software to imitate a legitimate software update on their computers. The students then asked teachers to enter administrative account information so that they could complete the software updates or installations. The phony software then stored teacher credentials. The students were then able to control 300 laptops belonging to other students by using the administrative credentials. The school believes that servers and sensitive information were not exposed. The breach occurred around Friday, April 26 and was discovered on Monday, April 29 when students noticed that other students appeared to be controlling student laptops remotely and reported the issue.

Information Source: California Attorney General

records from this breach used in our total: 0

April 12, 2013 **Chapman University**
Orange, California
EDU DISC Unknown

An administrative error caused the personal information of some students to be exposed online. The issue was discovered on February 27. Authenticated users of Chapman's on-campus network could have viewed names, Social Security numbers, student identification numbers, and dates of birth. The documents were blocked from access by unauthorized users once the breach was discovered.

Information

Source:
California
Attorney General

records from this breach used in our total: 0

April 11, 2013 **Chapman University**
Orange, California EDU DISC Unknown

Sensitive documents could have been viewed electronically by authenticated users of the on-campus network. The issue was discovered on February 27. Names, Social Security numbers, student identification numbers, and dates of birth may have been viewed by people who could log into Chapman's system, but shouldn't have been able to access the information.

Information Source:
California
Attorney General

records from this breach used in our total: 0

April 9, 2013 **Kirkwood Community College**
Cedar Rapids, Iowa EDU HACK 125,000

Hackers accessed Kirkwood Community College's website and applicant database system on March 13. Anyone who applied to a Kirkwood Campus may have had their names, Social Security numbers, dates of birth, race, and contact information exposed. People who applied to take Kirkwood college-credit classes between February 25, 2005 and March 13, 2013 were affected.

Information Source:
Media

records from this breach used in our total: 125,000

March 22, 2013 **University of Mississippi Medical Center (UMMC)**
Jackson, Mississippi EDU PORT Unknown

A laptop used by UMMC clinicians was discovered missing on January 22. The password-protected laptop contained information from patients who entered the hospital between 2008 and 2013. Patient names, Social Security numbers, addresses, diagnoses, medications, treatments, dates of birth, and other personal information may have been exposed.

UPDATE (04/25/2013): The laptop may have been lost or stolen in November of 2012.

Information Source:
Media

records from this breach used in our total: 0

March 22, 2013 **Tallahassee Community College (TCC)**
Tallahassee, Florida EDU HACK 3,300

Federal investigators informed Tallahassee Community College that a hacker gained access to their main computer system. The personal information of students who applied for financial aid may have been accessed. It appears that an insider hacked into the computer system. Hacked 2011 TCC financial aid records were misused to file fraudulent tax refunds. Federal Investigators told TCC when they traced where the information came from.

Information Source:
Media

records from this breach used in our total: 3,300

March 16, 2013 **Salem State University**
Salem, Massachusetts EDU HACK 25,000

A server was found to be infected with a virus. The University computer contained information related to paychecks distributed by the University. Current and former employees who may have been students or staff may have been affected.

Information Source: Media

records from this breach used in our total: 25,000

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

Capella University's official breach notice can be found here [8]: 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

Breach Total

621,061,494 RECORDS BREACHED

(Please see explanation [9] about this total.)
from 4,067 DATA BREACHES made public since 2005

Showing 43 results

Links:
[1] http://www.privacyrights.org/data-breach/new
[2] http://www.privacyrights.org/data-breach-how-to
[3] http://www.privacyrights.org/data-breach
[4] http://www.sachem.edu/home/pdf/QAData11192013.pdf
[5] http://police.msu.edu/crimealert10202013.asp
[6] http://www.vtnews.vt.edu/articles/2013/09/092413-hr-hrserver.html
[7] http://www.udel.edu/it/response/
[8] http://www.atg.state.vt.us/assets/files/Capella%20University%20Security%20Breach%20Notice%20to%20consumer.pdf
[9] http://www.privacyrights.org/data-breach-FAQ#2