Date Mad	School/Co	School or	City	State	Type of b	Public or	Total Rec
1/20/2016	Anna Mari	College/Un	Paxton	Massachus	DISC	Private	1,161
1/31/2017	Babson Co	College/Un	Wellesley	Massachus	HACK	Private	0
2/21/2017	Bentley Un	College/Un	Waltham	Massachus	HACK	Private	0
11/3/2005	Boston Col	College/Un	Boston	Massachus	HACK	Private	120,000
2/24/2020	Boston Col	School	Boston	Massachus	HACK	Public	0
10/7/2015	Boston Uni	College/Un	Boston	Massachus	HACK	Private	828
4/11/2015	Boston Uni	College/Un	Boston	Massachus	HACK	Private	0
###	Brandels U	College/Un	Waltham	Massachus	PORT	Private	0
7/6/2016	Cambridge	College/Un	Boston	Massachus	DISC	Private	9000
7/20/2018	Clark Univ	College/Un	Worcester	Massachus	HACK	Private	0
10/20/201	College of	College/Un	Worcester	Massachus	UNKN	Private	493
10/23/201	College of	College/Un	Worcester	Massachus	DISC	Private	0
5/21/2015	Diman Reg	School	Fall River	Massachus	DISC	Public	0
1/15/2017	Dracut Pub	School	Dracut	Massachus	HACK	Public	0
10/24/201	Endicott C	College/Un	Beverly	Massachus	HACK	Private	0
10/4/2015	Fitchburg	College/Un	Fitchburg	Massachus	DISC	Public	393
2/21/2017	Harvard C	College/Un	Cambridge	Massachus	DISC	Private	1400000
12/3/2008	Harvard U	College/Un	Cambridge	Massachus	HACK	Private	6,600
3/3/2005	Harvard U	College/Un	Cambridge	Massachus	HACK	Private	200
11/14/200	Harvard U	College/Un	Cambridge	Massachus	PHYS	Private	56
8/1/2008	Harvard U	College/Un	Cambridge	Massachus	INSD	Private	0
1/9/2011	Harvard U	College/Un	Cambridge	Massachus	DISC	Private	0
8/10/2012	Harvard U	College/Un	Cambridge	Massachus	HACK	Private	0
2/7/2015	Harvard U	College/Un	Cambridge	Massachus	HACK	Private	0
3/20/2008	Lasell Coll	College/Un	Newton	Massachus	HACK	Private	20,000
1/24/2016	Lawrence	School	Lawrence	Massachus	HACK	Public	0
2/16/2008	Malden Sc	School	Malden	Massachus	PORT	Public	233
11/23/201	MassBay C	College/Un	Wellesley	Massachus	DISC	Public	0
10/29/200	New Engla	College/Un	Boston	Massachus	DISC	Private	5098
2/10/2007	Pembroke	School	Pembroke	Massachus	DISC	Public	0
1/7/2017	Rising Tide	School	Plymouth	Massachus	HACK	Public	272
10/4/2015	Roxbury C	College/Un	Boston	Massachus	UNKN	Public	0
3/16/2013	Salem Stat	College/Un	Salem	Massachus	HACK	Public	25,000
2/14/2008	Springfield	School	Springfield	Massachus	PORT	Public	38
7/16/2013	Suffolk Uni	College/Un	Boston	Massachus	HACK	Private	0
11/4/2005	Tufts Unive	College/Un	Medford	Massachus	HACK	Private	106,000
5/21/2010	Tufts Unive	College/Un	Medford	Massachus	HACK	Private	2,000
7/31/2011	Tufts Unive	College/Un	Medford	Massachus	PORT	Private	73
8/21/2009	University	College/Un	Amherst	Massachus	HACK	Public	0
10/3/2011	University	College/Un	Amherst	Massachus	HACK	Public	0
1/30/2008	University	College/Un	Dartmouth	Massachus	DISC	Public	32
1/24/2011	Wentworth	College/Un	Boston	Massachus	DISC	Private	1300
2/19/2019	Wenworth	College/Un	Boston	Massachus	HACK	Private	3926
10/30/200	Williams C	College/Un	Williamsto	Massachus	PORT	Private	750

Informati	**Year of B**	**Description of incident**
ITRC	2015	An employee intended to send an email to a student with the stu
ITRC	2017	Phishing scam.
ITRC	2017	Phishing scam.
Dataloss D	2005	A hacker gained access to a phone banking database that include
ITRC	2019	Phishing email.
ITRC	2015	In May 2015, a member of the staff of Boston University's Inform
ITRC	2015	I am writing to inform you of a data security incident at Boston U
ITRC	2015	Two Apple laptops containing academic and personal information
ITRC	2016	The MacKeeper Security Research center experts have discovere
ITRC	2018	Phishing attack.
Databreacl	2011	Seven Holy Cross employees fell for phishing attempts.Â The em
ITRC	2017	On September 22nd, 2017, a Col!ege employee accidentally cros
ITRC	2015	Diman Regional Vocational Technical High School ("Diman") is wri
ITRC	2017	Employees of Dracut Public Schools in Massachusetts weren’t as
ITRC	2019	Suspicious email activity from an email account belonging to a th
ITRC	2015	A student notified the school that they were able to see and dow
ITRC	2017	More than 1.4 million emails were open to the public.
Dataloss D	2008	Harvard Graduate School of Arts and Sciences (GSAS) Web serve
ITRC	2005	Intruder gains access to admission systems at Harvard, Stanford
Dataloss D	2007	Folders containing information about students from the Universit
ITRC	2008	Harvard University police and the Middlesex district attorney's of
Databreacl	2011	Harvard's switch to Google "@college" email accounts resulted in
Databreacl	2012	A hacking group called Team GhostShell targeted universities aro
Media	2015	"Last month Harvard University uncovered "an intrusion" on its c
Dataloss D	2008	A hacker accessed data containing personal information on curre
ITRC	2016	Hackers breached Lawrence Public Schools’ online database, acq
ITRC	2008	A hard drive containing the names and Social Security numbers c
Databreacl	2011	A glitch allowed nearly 400 workers from 2002 to 2011 to view th
ITRC	2007	In mid-October, the New England School of Law was alerted that
ITRC	2007	Anyone who worked for or volunteer for the Pembroke schools in
ITRC	2017	On February 13, 2017, we discovered that cyber attackers may h
ITRC	2015	The attorney general’s office is investigating a data breach at Ro
Media	2013	A server was found to be infected with a virus. Â The University c
ITRC	2008	The Springfield Police Department is investigating the theft of thr
ITRC	2013	Suffolk University was recently contacted about a potential breac
Dataloss D	2005	The University's donor database was breached sometime in late
Databreacl	2010	Campus computers with former student files were exposed to a v
ITRC	2011	A research associate's laptop was stolen during the course of res
Dataloss D	2009	Nearly a year ago, hackers broke into a computer server that con
PHIPrivacy.	2011	A workstation at the campus University Health Services (UHS) wa
Dataloss D	2008	A privacy organization discovered the names, grades, GPAs and p
ITRC	2011	WIT's system was inadvertently put online. The letter said that a
ITRC	2018	Phishing attack.
ITRC	2009	Williams College in Williamstown reports a recent laptop theft. Th

dent's financial statement, but because of a software error the attachment actually cor

ed alumni addresses and Social Security numbers.

ation Systems & Technology Department (IS&T) was contacted by the administrator of a
niversity related to your participation in the Boston University Initiative for Literacy Dev
for all students enrolled or taking a course at the University from the summer of 2012
d and helped to secure a publicly available, non-password protected database containir

ployees had their email accounts attacked and emails containing personal information
s-mailed promissory notes of at least 4, and as many as 28 College alumni via the Unit
iting to provide notice of a data security incident that may affect the security of some c
fortunate as those at Kanawha County Schools in West Virginia. Rick Sobey and Todd Fe
ird-party educational institution.
nload an Excel spreadsheet that contained PII while they were searching Google Drive c

r may have compromised 10,000 sets of personal information from applicants and stud
and other top business schools and helped applicants log on to learn whether they had
y's Division of Continuing Education were lost. The folders were from the previous year
fice are investigating a security breach at the school after an undergraduate allegedly r
the potential compromise of some student emails. Â Fewer than ten students reportec
und the world. Â A total of 53 universities were affected. Â Most of the data exposed wa
omputer networks,Â the school disclosedÂ late Wednesday."The discovery, which was r
nt and former students, faculty, staff and alumni. Information included names and Soci
uiring teachers' personal information, possibly including their Social Security numbers,
of more than 263 teachers, state employees, and consultants vanished from the School
e personal information of any employees in MassBay's worker database system.Â The
personal information, including SSNs, of school alumni was available on a page of the s
the last four years has been exposed to a data breach that includes, names and SSNs.
ave gained unauthorized access to information stored on a computer server utilized by
xbury Community College, the school's president said in an e-mail to the college comm
computer contained information related to paychecks distributed by the University. Â Cu
ee laptop computers in eight days from the Springfield School Department's central off
h of personal information through its third-party ticketing vendor, Vendini, Inc. Vendini
2004. Â The database was managed by a software company for nonprofit organizations
irus.Â Over two thousand alumni may have had their Social Security numbers and oth
earch with a Tufts professor. Â The research was being conducted at MGH. Â The laptop
tained Social Security numbers and a very limited amount of credit card information fo
s infected with malware. The work station contained patient names, health insurance c
partial Social Security numbers of 32 former students. It appears that the information is
"electronic file was accessible on the Institute's website that contained personal infor

e laptop, which was stolen when an employee left it in a parked car in Boston on Octob ntained the 1098T forms of 1590 students at the college.

a network in Halifax, Nova Scotia who reported that a server on the Boston University n
velopment ("BUILD") program through the University's School of Education. Boston Univ
to the present were stolen from the University Registrar, according to a Nov. 12 email s
ng more than a half of a million records on international students and info on 12 thousa

for hundreds of people were exposed.Â Though Holy Cross has a policy of encrypting a
ed States Postal Service (1 of those being a resident of New Hampshire).
of your personal information. What happened? On May 4, 2015, an email with an attach
eathers report that current and former employees’ personal information, including SSN,

on the student domain. (Reported to MA Office of Consumer Affairs 4/10/2015)

ents, including 6,600 Social Security numbers and 500 Harvard ID numbers.
been accepted weeks before they were to find out. “Dozens of business schools (list of
and included names, Social Security numbers, Harvard ID numbers, dates of birth, add
manufactured phony driver's licenses and university identification cards that can be use
that emails from other students with similar names were forwarded to them. Â The pro
as publicly available, but student, staff, and faculty usernames and passwords were als
nade June 19, affects two IT systems that impact eight colleges and administrations, th
al Security numbers.
school officials said. In the email, Riley said the breach may have disclosed employees
Department earlier this week, baffling officials. An auditor at the Department of Educa
information included Social security numbers, home addresses, and other personnel in
school's website through the Internet search engine Google." It has been removed
It was available on the Internet from May until October 2, 2007. School officials attribut
the School. The information potentially accessed may have included your name, addre
unity on Thursday. President Valerie Roberson did not disclose the nature of the breach
urrent and former employees who may have been students or staff may have been affe
fice. The thefts began on 2/7 and at least one computer had names and SSNs of 38 sch
has reported that, on April 25, 2013, the company detected an unauthorized intrusion i
named RuffaloCODY. Â Letters were sent to the alumni who may have had their persor
er information exposed.
was mostly used for research, but a sensitive file had been uploaded in early 2010. Â I
r graduates of University of Massachusetts. Hackers gained access to one server on the
company names, medical record numbers, and prescription information from January 2,
from a Fall of 2004 CIS 100 class. The discovery was made in December and all affecte
mation for a group of current and former students, including full name, social security r

ber 3, contained the names and Social Security numbers of 750 individuals from 39 stat

ıetworks (the "Server'') was attacking the system in Nova Scotia. As a result of this repo
/ersity recently learned that an email account connected with the BUILD program was a
sent by Marianne Cwalina, the senior vice president for finance and treasurer. One of th
nd host families and housing information

ıll emails that contain personal information, these emails were not encrypted.Â Those

ed spreadsheet containing personal information was inadvertently sent by an employe
was acquired by a hacker after an employee fell for what the district describes as a "sc

f some schools) were affected by the breach, with their web sites vulnerable for roughly
resses, email addresses and phone numbers. Some of the folders contained additional
ed as debit cards and to enter residence halls, the university announced yesterday. The
oblem occurred because the email system did not distinguish between the older "@fas'
o exposed. It is unclear if any financial information or Social Security numbers were tak
e school says. These include the Faculty of Arts and Sciences, Harvard Divinity School,

' names, phone numbers, addresses, Social Security numbers and calendar year 2015 (
tion's Malden headquarters arrived at work Tuesday to find his computer wasn't workin
ıformation.Â

ted the security breach to a problem with data storage within the district's computer sy
ess, date of birth and Social Security Number
, which was discovered around March 16. It was reported to the board of trustees, the s
cted.
ool teachers.
into its systems. If you used your credit card to make a purchase for a Suffolk Universit
ıal information stolen.

t contained a spreadsheet with the information of applicants who applied to the Gradua
e university's computer system, which held information of students who attended UMas
2009 to November 17, 2009. There is no evidence that the data was copied from the w
ed students were informed by March 3 of 2008.
ıumber, and date of birth.

tes and several foreign countries. They did not state if these individuals were former or

ɔrt, the University's Information Security Department initiated an investigation. During
ıccessed without authorization. That account contained certain forms related to the Bos
e stolen computers contained students' "names, birth dates, permanent and email add

who could have been affected were notified that their Social Security numbers, driver's

e in Diman's Human Resources Department to all faculty. The email was recalled that sa
ɔphisticated phishing scheme."

/ nine hours before the problem was fixed."
information about the students and their dependents, spouses or parents. The informat
cards, which have a magnetic strip on them, are issued to Harvard students, faculty, a
' accounts and the newer "@college" accounts. Â For example, the system would forwa
ɛen from universities.
Radcliffe Institute for Advanced Study, Central Administration, the Graduate School of [

gross earnings. However, the breach did not include any employees' bank account infor
g. Technical workers identified the problem: His hard drive was missing. Someone had t

stem.

state Department of Higher Education and Attorney General Maura Healy's office, Rober

/ event through Vendini prior to April 25, 2013, your information, including your credit c

ate School of Arts and Sciences at Tufts. Â Applicant Social Security numbers were inclu
s between 1982 and 2002, as well as a few who attended before 1982. A UMass spokes
vorkstation. The malware was on the computer from June 30, 2010 to October 28, 2010

current students or employees.

the more than month-long complex investigation, investigators learned that a third par
ston Public Schools' criminal background check process for participants in the BUILD pro
resses, phone numbers, courses, and grades," according to Cwalina's email, which wer

license numbers, dates of birth, financial information and other types of information w

ame day, but some individuals had already received the email.

tion did not include credit card numbers. The University speculates that the folders wer
nd staff members and are encoded with an identification number. A person can put mo
rd emails from ctucker@fas.harvard.edu to the new address of ctucker@college.harvar

Design, Harvard Graduate School of Education, Harvard John A. Paulson School of Engin

rmation, according to Rile
taken it.

rson said. Authorities went to the campus Thursday morning to collect evidence and to

card number, may have been compromised.

ded in the spreadsheet. Â The theft occurred in April of 2011 and was reported to MGH.
sman declined to say how many people's records were exposed, except that it was a la
. Patients were notified in March.

ty had infiltrated the Server and had installed a hacking toolkit, which was responsible
ogram (the "CORI forms"), one of which included your name, social security number and
nt out to students, faculty and staff. “It is also possible that this device contained some

were at risk.Â

e placed in a file cabinet that was later recycled.
oney on the ID cards, called Crimson Cash, and use them like a debit card to purchase it
d.com even if the "@harvard" email had been taken by a different student. Students wi

eering and Applied Sciences, or Harvard T.H. Chan School of Public Health."

interview college employees as part of an ongoing investigation.

. Â Tufts learned of the breach on June 16, 2011.
rge number of undergraduate and graduate students who attended the university durin

for the attacks on the system in Nova Scotia.
d driver's license number.
Social Security numbers,” according to the email.

tems at stores on and off campus, buy items at campus vending machines, pay for cam
th "@harvard" emails also had their emails forwarded to other students'Â accounts.

ng the 20-year period.

pus laundry machines, and gain access to residence and dining halls.