Breached: A chronology of every major data breach since 2005

If you were asked to guess how many personal data records (containing social security numbers, credit card information, and so on) had been breached since 2005, what would you say?

A million? 50 million? 100 million? How about almost three times the population of the United States: 930 million. That is the actual minimum number of records since 2005 that have been stolen, leaked, lost or otherwise disclosed by hackers, insiders, careless employees and unscrupulous data brokers.

It's a number so mind-bogglingly massive that it almost loses any sense of meaning. But the effect of every breach is eventually felt by consumers. The tech company Symantec estimated in 2013 that the average cost of a data breach per consumer was about $200. Not every person whose records are compromised will be end up being a victim, but it's becoming increasingly likely that they will. In 2010, if you received a notification of a data breach, your chances of becoming a victim of fraud were one in nine. By 2012, those odds had shrunk to one in four. Now, in 2014, it's one in three.

With new data breaches hitting the headlines on an almost daily basis—and Morgan & Morgan on the frontlines of the litigation—we thought we'd chart their history over the last nine years, including which companies, organizations and government departments were hit; what data was taken; how the data was compromised and what the knock-on effects were for consumers.

Jump to:

- ▶ Top 10 data breaches since 2005
- ▶ Data breaches by U.S. states (All - Financial - Retail - Education - Government - Medical - Non-profit)
- ▶ Top 10 university data breaches since 2005
- ▶ Top 25 data breaches tree map

The graphic below details every major data breach since 2005 (which we have defined as involving more than 50,000 records). There are 346 of them, color-coded by the way the data was breached (hack, insider, etc.). The breaches are placed according to the date they were first announced, because the actual dates are almost always unknown, even by the companies involved. All graphics from this point forward were made using data from Privacy Rights Clearinghouse's excellent online database of breaches.

A Chronology of Major Data Breaches Since 2005

50k
500k
1m
1.5m
2m
2.5m
3m
3.5m
4m
4.5m
5m
5m
25m
45m
65m
85m
105m
125m
145m
165m
185m
200m
Total records across all breaches
Entity with most breached records
Key
k = thousand records
m = million records
Bar color denotes type of data breach
Hack/malware
Portable media
Insider
Unintended disclosure
Physical loss
Payment card fraud
Non-portable
Unknown
Only breaches with more than 50,000 individual persons' records compromised are included. Bars on the chart show total records breached on each day and the entity responsible for the majority of them.
2005
Feb '05
Insider 163k - ChoicePoint
Portable Media 1.2m - Bank of America Corp.
Hack 1.4m - DSW Shoe Warehouse
Mar '05
Insider 310k - LexisNexis
Hack 120k - Boston College
Hack 59k - California State University, Chico
Apr '05
Non-Portable 187k - San Jose Medical Group
Hack 106k - Tufts University
Hack 180k - Polo Ralph Lauren, HSBC
Portable Media 200k - TD Ameritrade
Hack 40k - Michigan State University's Wharton Center
Insider 676k - Wachovia, Bank of America, PNC, et al.
May '05
Portable Media 600k - Time Warner, Iron Mountain Inc.
Portable Media 80k - Department of Justice
Insider 465k - Georgia Technology Authority (GTA)
Jun '05
Portable Media 3.9m - Citigroup
Hack
Insider 50k - University of Hawaii
Hack 72k - University of Connecticut (UCONN)
Jul '05
Disclosure 270k - University of Southern California (USC)
Portable Media 57k - Arizona Biodyne
Aug '05
Hack 100k - University of Utah
Sep '05
Portable Media 165k - Iowa Student Loan
Non-Portable 100k - Kent State University
Oct '05
Portable Media 130k - Wilcox Memorial Hospital
Nov '05
Non-Portable 50k - Keck School of Medicine, USC
Portable Media 161k - Boeing
Dec '05
Portable Media 100k - First Trust Bank
Non-Portable 70k - Ford Motor Co.
Portable Media 262k - Ameriprise Financial Inc.
Portable Media 206k - Marriott International Inc.
2006
Jan '06
Portable Media 90k - People's Bank
Portable Media 365k - Providence Home Services
Disclosure 240k - Boston Globe and The Worcester Telegram
Feb '06
Hack 200k - OfficeMax
Disclosure 350k - U.S. Department of Agriculture (USDA)
Mar '06
Hard Copy 2m - L.A. County DPSS
Portable Media 93k - Metropolitan State College of Denver (MSCD)
Portable Media 84k - Ernst & Young, IBM
Portable Media 196k - Fidelity Investments
Disclosure 64k - California State Employment Development Division
Apr '06
Hack 573k - Georgia Technology Authority (GTA)
Hack 197k - University of Texas McCombs School of Business
Portable Media 93k - Pershing LLC
May '06
Hack 137k - Ohio University
Hack 70k - Ohio University Hudson Health Center
Portable Media 330k - American Institute of Certified Public Accountants
Insider 1m - American Red Cross, St. Louis Chapter
Portable Media
Insider 231k - Mortgage Lenders Network USA
Unknown 1.7m - Texas Guaranteed Student Loan
Jun '06
Portable Media 243k - Ernst & Young
Portable Media 92k - Ahold USA
Portable Media 72k - Buckeye Community Health Plan
Hard Copy 150k - Denver Election Commission
Non-Portable 930k - American International Group (AIG), et al.
Hack 180k - Western Illinois University
Hack 309k - Nebraska Treasurer's Office
Unknown 41k - National Institutes of Health Federal Credit Union
Jul '06
Portable Media 61k - Bisys Group Inc.
Disclosure 100k - Naval Safety Center, United States Navy
Non-Portable 722k - CS Stars
Portable Media 23k - Georgetown University Hospital
Insider 112k - Sentry Insurance
Aug '06
Hard Copy 51k - PSA HealthCare
Portable Media 132k - U.S. Department of Transportation
Portable Media 2.6m - Circuit City
Sep '06
Hack 64k - University of Texas San Antonio
Portable Media 50k - General Electric (GE)
Disclosure 146k - Kentucky Personnel Cabinet via Bluegrass Mailing
Oct '06
Disclosure 1.35m - Chicago Voter Database
Hack 236k - Akron Children's Hospital
Non-Portable 332k - Link Staffing Services
Nov '06
Non-Portable 1.4m - CDHS
Portable Media 60k - Starbucks Corp.
Non-Portable 300k - Look Tours LLC
Non-Portable 101k - Greenville County School District
Dec '06
Hack 800k - University of California at Los Angeles
Portable Media 382k - Boeing
Portable Media 63k - Electronic Registry Systems
2007
Jan '07
Disclosure 171k - Wisconsin Department of Revenue via Ripon Printers
Insider 300k - Towers Perrin
Non-Portable 70k - University of Idaho
Hack 79k - MoneyGram International
Hack
Portable Media 1.3m - Chicago Board of Election
Portable Media 50k - WellPoint's Anthem Blue Cross Blue Shield
Hack 70k - Vermont Agency of Human Services
Feb '07
Portable Media 583k - U.S. Department of Veterans Affairs
Hack 130k - Merchant America
Portable Media 135k - Johns Hopkins University and J.H. Hospital
Portable Media 130k - St. Mary's Hospital
Disclosure 65k - East Carolina University
Hack 77k - State of Indiana Official Website www.IN.gov
Mar '07
Portable Media 63k - ADC Telecommunications Inc., Flex Compensation
Portable Media 75k - WellPoint's Empire Blue Cross, et al.
Portable Media 243k - Los Angeles County Child Support Services
Portable Media 268k - Hortica, UPS
Apr '07
Portable Media 2.9m - Georgia DCH
Hard Copy 75k - Georgia Secretary of State
Non-Portable 60k - Neiman Marcus Group
May '07
Portable Media 100k - Transportation Security Administration (TSA)
Hack 197k - Community College of Southern Nevada
Hack 140k - Georgia Division of Public Health
Hack 300k - Illinois Dept. of Financial and Professional Reg.
Hack 45k - University of Colorado, Boulder
Jun '07
Portable Media 1m - Ohio state workers
Disclosure 65k - Milwaukee PC
Jul '07
Insider
Portable Media 100k - Transportation Security Administration (TSA)
Disclosure 80k - Louisiana Board of Regents
Disclosure 867k - Science Applications International Corp.
Disclosure 51k - St. Vincent Hospital, Verus, Inc.
Portable Media 70k - Yuba County Health and Human Services
Aug '07
Disclosure 445k - California Public Employees' Retirement System
Portable Media 106k - Connecticut Department of Revenue Services
Non-Portable 69k - McKesson Specialty, AstraZeneca
Non-Portable 112k - Gander Mountain
Sep '07
Portable Media 67k - TennCare, Americhoice Inc.
Hack
Oct '07
Portable Media 800k - Gap Inc.
Disclosure 450k - Massachusetts Division of Professional Licensure
Portable Media 159k - Administaff Inc.
Portable Media 200k - West Virginia Public Employees Insurance Agency
Portable Media 230k - Hartford Financial Services Group
Nov '07
Insider 185k - U.S. Department of Veteran Affairs
Unknown 150k - Prescription Advantage
Dec '07
Portable Media 268k - Memorial Blood Centers
Portable Media 337k - Davidson County Election Commission
2008
Jan '08
Portable Media 80k - Mariner Health Care, Windham Brannon, et al.
Disclosure 260k - Wisconsin Department of Health & Family Services
Portable Media 150k - GE Money, Iron Mountain
Non-Portable 35k - T. Rowe Price Retirement Plan Services, CBIZ
Portable Media 300k - Horizon Blue Cross Blue Shield
Hack 226k - Davidson Companies
Feb '08
Portable Media 321k - Lifeblood
Disclosure 103k - Health Net Federal Services
Mar '08
Hack
Disclosure 74k - The Dental Network
Disclosure 30k - Pennsylvania Department of State
Insider 1m - Compass Bank
Portable Media 51k - Agilent Technologies
Portable Media
Apr '08
Hack 70k - Antioch University
Hack 56k - Advance Auto Parts
Portable Media 60k - Harley-Davidson, Inc. (HOG)
Disclosure 128k - WellPoint
Portable Media 2.1m - University of Miami
Non-Portable 700k - Central Collection Bureau
Portable Media 200k - CollegeInvest
May '08
Non-Portable 88k - Staten Island University Hospital
Hack 80k - Dave & Buster's
Hack 70k - Oklahoma State University
Hack 55k - Chester County School District
Jun '08
Portable Media 72k - Stanford University
Portable Media 1.3m - University of Utah Hospitals and Clinics
Portable Media 70k - Aon Consulting
Hack 51k - Montgomery Ward
Jul '08
Disclosure 55k - Florida Agency for Health Care Administration
Disclosure 3.4m - DMV Colorado
Portable Media 42k - Bristol-Myers Squibb
Hack 128k - Saint Mary's Regional Medical Center
Disclosure 202k - Blue Cross and Blue Shield of Georgia
Aug '08
Insider
Hack 92k - Dominion Enterprises
Sep '08
Hack 99k - Forever21
Insider 89k - Texas Lottery Commission
Oct '08
Portable Media 85k - University of North Dakota Alumni Association
Portable Media 100k - Baylor Health Care System Inc.
Nov '08
Unknown 700k - Express Scripts
Hack 330k - University of Florida College of Dentistry
Portable Media 97k - Starbucks Corp.
Hack 59k - Luxottica Group, Things Remembered
Dec '08
Disclosure 259k - Florida Agency for Workforce Innovation
Portable Media 69k - DJO, Empi Recovery Services
Hack 1.1m - RBS WorldPay
2009
Jan '09
Hack 5m - CheckFree Corp
Hack
Feb '09
Hack 48k - Federal Aviation Administration
Hack 97k - University of Florida
Portable Media 807k - Arkansas Department of Information Systems
Mar '09
Insider 800k - New York Police Department
Portable Media 59k - Idaho National Laboratory
Non-Portable 100k - Binghamton University
Portable Media 63k - Dezonia Group
Apr '09
Portable Media 100k - Peninsula Orthopaedic Associates
Portable Media 1m - Oklahoma Department of Human Services
Portable Media 225k - Oklahoma Housing Finance Agency
Hack 531k - Virginia Prescription Monitoring Program
May '09
Hard Copy 99k - Fulton County Board of Registration and Elections
Hack 160k - University of California, Berkeley
Portable Media 250k - National Archives and Records Administration
Hack 65k - Aetna
Jun '09
Portable Media 84k - Blackbaud Inc.
Jul '09
Hack 573k - Network Solutions
Aug '09
Portable Media 131k - National Guard Bureau
Sep '09
Hack 52k - Mitsubishi Corp.
Hack 163k - University of North Carolina, Chapel Hill
Oct '09
Portable Media
Portable Media 187k - BlueCross BlueShield Assn.
Portable Media 103k - Virginia Department of Education
Portable Media 68k - CalOptima
Nov '09
Non-Portable 250k - National Archives and Records Administration
Portable Media 1.5m - Health Net
Dec '09
Hack 51k - North Carolina Libraries
Hack 130k - Eastern Washington University
2010
Jan '10
Insider 1.2m - Lincoln National Corporation
Disclosure 75k - University of Missouri System
Unknown 77k - PricewaterhouseCoopers
Hack 80k - Iowa State Racing and Gaming Commission
Feb '10
Portable Media 1.22m - AvMed Health Plans
Disclosure 50k - California Department of Health Care Services
Hack 170k - Valdosta State University
Disclosure 600k - Citigroup
Hack 500k - Wyndham Hotels & Resorts
Mar '10
Portable Media 3.3m - ECMC
Apr '10
Portable Media 409k - Affinity Health Plan
May '10
Portable Media 180k - Millennium Medical Management Resources
Portable Media 207k - Army Reserve/Serco Inc.
Jun '10
Hack 200k - Digital River Inc.
Disclosure 470k - Anthem Blue Cross, WellPoint
Portable Media 130k - Lincoln Medical and Mental Health Center
Jul '10
Non-Portable 79k - AMR Corporation
Portable Media 79k - AMR Corporation
Hard Copy 39k - Massachusetts Secretary of State Office
Portable Media 139k - Massachusetts Secretary of State, Securities Division
Portable Media 378k - Marsh and Mercer
Hack 93k - Buena Vista University
Aug '10
Disclosure 126k - College Center for Library Automation (CCLA)
Oct '10
Hack 53k - University of North Florida
Hack 56k - Emergency Medical Services Bureau
Dec '10
Hack 60k - University of Wisconsin - Madison
Hack 750k - Ohio State University
Hack 110k - Twin America LLC, CitySights NY
2011
Jan '11
Hack 231k - Seacoast Radiology
Hack 156k - Ankle and Foot Center of Tampa Bay, Inc.
Feb '11
Portable Media 1.7m - Jacobi Medical Center, et al.
Portable Media 400k - Cambridge Who's Who Publishing, Inc.
Mar '11
Portable Media 300k - Cord Blood Registry
Portable Media 1.9m - Health Net Inc., et al.
Non-Portable 514k - Eisenhower Medical Center (EMC)
Apr '11
Portable Media 94k - MidState Medical Center
70k - Family Planning Council
Disclosure 3.5m - Texas Comptroller's Office
Portable Media 133k - Oklahoma State Department of Health
Disclosure 64k - Social Security Administration (SSA)
Hack
May '11
Card 94k - Michaels Stores Inc.
Hack 210k - Massachusetts EOLWD
Portable Media 400k - Spartanburg Regional Hospital
Jun '11
Hack 360k - Citibank
Disclosure 300k - Southern California Medical-Legal Consultants, Inc.
Jul '11
Hack 142k - Kiplinger Washington Editors Inc.
Aug '11
Hack 79k - University of Wisconsin - Milwaukee
Disclosure 92k - Lincoln Financial Group, et al.
Sep '11
Hack 72k - El Paso Independent School DIstrict (EPISD)
Portable Media 5.12m - TRICARE Management Activity, Science Applications
Oct '11
Portable Media 1.6m - The Nemours Foundation
Portable Media 63k - Neurological Institute of Savannah and Center for Spine
Nov '11
Hack
Hack 177k - Virginia Commonwealth University
Dec '11
Hack 80k - Subway
Hack 300k - Restaurant Depot, Jetro Cash & Carry
Hack 68k - Stratfor.com, Strategic Forecasting Inc.
2012
Jan '12
Disclosure 1.25m - New York State Electric & Gas, et al.
Feb '12
Disclosure 350k - University of North Carolina at Charlotte
Disclosure 50k - Piedmont Behavioral Healthcare (PBH), et al.
Mar '12
Portable Media 67k - Howard University Hospital
Portable Media 800k - Department of Child Support Services, et al.
Card
Apr '12
Hack 280k - Utah Department of Health
Hack 88k - Housatonic Community College
Portable Media 228k - Emory Healthcare, Emory University Hospital
Disclosure
May '12
Disclosure 100k - Florida Department of Children and Families
Portable Media 701k - Hewlett Packard, California DSS
Hack 654k - University of Nebraska, et al.
Jun '12
Disclosure 95k - Franklin's Budget Car Sales, Inc.
Disclosure 86k - Bethpage Federal Credit Union
Jul '12
Disclosure 111k - Wisconsin Department of Revenue
Aug '12
Insider 102k - Memorial Healthcare System (MHS)
Portable Media 66k - Apria
Portable Media 55k - Cancer Care Group
Sep '12
Insider 65k - University of Miami Health System
Oct '12
Portable Media 260k - TD Bank
Hack 200k - Northwest Florida State College
Hack
Nov '12
Portable Media 100k - Alere Home Monitoring, Inc.
Hack 1m - Nationwide Mutual Insurance Company, et al.
Disclosure 235k - Western Connecticut State University
2013
Jan '13
Portable Media 300k - Cbr Systems
Feb '13
Hack 110k - Central Hudson Gas & Electric
Non-Portable 100k - Crescent Health Inc., Walgreens
Apr '13
Hack 125k - Kirkwood Community College
May '13
Hack 160k - Administrative Office of the Courts - Washington
Hard Copy 189k - El Centro Regional Medical Center
Insider 56k - RentPath, Inc. (Primedia)
Jul '13
Disclosure 146k - Citigroup
Hack 116k - St. Mary's Bank
Hack 74k - University of Delaware
Aug '13
Hack 70k - Northrop Grunman
Unknown 104k - U.S. Department of Energy
Hack 120k - League of Legends, Riot Games
Non-Portable 4m - Advocate Medical Group
Portable Media 82k - Republic Services
Oct '13
Unknown 74k - Comcast Phone
Hack 2.9m - Adobe
Disclosure
Portable Media 73k - AHMC Healthcare, Inc.
Nov '13
Hack 850k - CorporateCarOnline.com
Unknown 2.49m - Maricopa County Community College
Hack 90k - University of Washington Medicine
Dec '13
Hack 465k - JPMorgan Chase
Portable Media 840k - Horizon Healthcare Services, Inc.
Hack
2014
Jan '14
Hack 1.1m - Neiman Marcus
Hack 2.6m - Michaels Stores Inc.
Feb '14
Hack 405k - St. Joseph Health System
Hack 309k - University of Maryland
Hack 146k - Indiana University
Mar '14
Hack 291k - North Dakota University
Apr '14
Hack 55k - Veterans Of Foreign Wars Of The United States
Hack 400k - Aaron Brothers
May '14
Hack 233k - Paytime
Hack 50k - Arkansas State College of Education...
Jun '14
Hack 120k - Splash Car Wash
Hack 163k - Butler University
Jul '14
Hack 868k - Goodwill Industries International Inc.
Hack 73k - Total Bank
Aug '14
Hack 4.5m - Community Health Systems
Hack 1m - J.P. Morgan Chase
Sep '14
Hack
Hack 5k - Bartell Hotels

CardSystems Solutions

Method: Hack Attacker: At large

The 16th of June 2005 saw the discovery of the then largest computer hack in history. The breach proved to be CardSystems Solutions' downfall and the company was sold within six months of the discovery.

Records breached **40m** News stories **12k**

L.A. County DPSS

Method: Employee Culprit: Veronica Niko

Niko, a receptionist at the L.A. County Department of Public Social Services, stole the information of up to 2 million people who had filed tax returns with the DPSS. She used the information together with her husband, Thomas Marshall, to file fraudulent tax returns costing the IRS $357,705.

Records breached **2m** Est. cost to the IRS **$358k**

U.S. Dept. of Veterans Affairs

Method: Burglary Culprit: At large

On May 3rd 2006, the residence was burglarized of an employee who had taken his company laptop and hard disc drive home.

The robbery, which included the laptop, led to the breach of 26.5 million veterans' records.

Records breached **26.5m** Cost to U.S. Treasury **$20m**

Chicago Voter Database

Method: Theft Culprit: At large

The Chairman of the Board of Elections ordered a computer forensics audit, which led to the theft of the personal information from 1.35 million voters.

Boeing

Method: Theft Culprit: At large

Aircraft giant Boeing suffered the theft of a company-owned laptop containing the names, credit card information and other sensitive data of 382,000 Boeing workers and retirees.

TJ Maxx Stores

Method: Hack Attacker: Albert Gonzalez

The home and clothing retail giant saw one of the largest computer hacks in history when hackers gained access to more than 100 million customer records including credit and debit card information.

Records breached **100m** Est. cost to TJ Maxx Stores **$118m**

Fidelity National Info Services

Method: Employee Culprit: William Sullivan

Records breached **8.5m** Compensation paid to victims **$2m**

TD Ameritrade Holding Corp.

Method: Hack Attacker: At large

Records breached **6.3m** Compensation paid to victims **$50-$2.5k**

Gap Inc.

Method: Theft Culprit: At large

Records breached **800k** Compensation paid to victims: a year's free credit monitoring and fraud resolution assistance.

Hannaford Bros. Grocery Chain

Method: Hack Attacker: At large

Credit and debit card numbers were stolen during the card authorization process and 4.2 million unique card numbers were exposed.

Records breached **4.2m** Known cases of fraud from stolen records **1.8k**

Bank of New York Mellon

Method: Theft Culprit: At large

When an unencrypted backup tape went missing from the Bank of New York Mellon, it potentially exposed the personal information of 12.5 million customers.

Records breached **12.5m** Average cost to consumer **$197**

TD Ameritrade Holding Corp.

Method: Theft Culprits: At large

Records breached **3.4m** Thirty three potential suspects had access to the stolen data.

Countrywide Financial Corp.

Method: Theft Culprit: Rene L. Rebollo Jr

Employee Rene L. Rebollo Jr downloaded customer files, including Social Security numbers, from the company's computers onto thumb drives and sold the information to employees of other mortgage lenders for use as sales leads.

Records breached **17m** Compensation paid to victims: a year's free credit monitoring and fraud resolution assistance.

Heartland Payment Systems

Method: Hack Attacker: Albert Gonzalez

Albert Gonzalez, famed for the TJ Stores hack, was responsible for stealing customer data and credit and debit card information which allowed him and his accomplices to clone the information onto counterfeit cards. At the time, it was characterized as the largest ever criminal breach of card data.

Records breached **130m** Est. cost to Heartland Payment Services **140m**

Hacker Albert Gonzalez is accused of the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from 2005 through 2007.

U.S. Military Veterans

Method: Theft Culprit: At large

A hard drive sent out for repair led to the loss of 76 million U.S. Military Veterans' records.

Records breached **76m**

Lincoln National Corporation

Method: Theft Culprit: At large

Employees at Lincoln National were readily able to access the personal data of up to 1.2m customers.

Records breached **1.2m**

ECMC

Method: Theft Culprit: At large

ECMC, a company that guarantees federal student loans lost the personal data of up to 3.3 million people nationwide when a 'portable media device' went missing from their Minnesota offices. The lost data included names, addresses, DOB and social security numbers for student loan borrowers across the country.

Records breached **3.3m**

Ohio State University

Method: Hack Attacker: At large

Around 750k students and professors had their names and Social Security numbers compromised.

Est. cost of investigation & credit-protection services **$4m**

Sony PlayStation Network

Method: Hack Attacker: At large

The breach which caused Sony to shut down the PSN for 7 days was originally reported as containing 77 million names, addresses and credit card numbers. That number later fell to 12m after an investigation.

Records breached **12m** Est. cost to Sony in compensation paid **$15m**

Steam - The Valve Corporation

Method: Hack Attacker: At large

In the second game industry related breach of the year, the Steam Network hack compromised the personal information of up to 35 million Steam/Valve customers.

Records breached **35m** Compensation paid to consumers **$0**

Subway

Method: Hack Attackers: Incarcerated

Records breached **80k**

Global Payment

Method: Card Culprit: At large

Records breached **7m**

Office of the Texas Attorney General

Method: Release of discs

The Office of the Texas Attorney General released discs containing information for over 13m Texas residents. Half were encrypted but mistakenly 6.5m remained readable and contained SS numbers.

Records breached **6.5m**

South Carolina Department of Revenue

Method: Hack Attacker: At large

A major hack which led to 3.8 million tax payers and their 1.9 million dependents losing Social Security numbers, credit and debit card information and bank account details.

Records breached **6.4m**

Court Ventures owned by Experian

Method: Disclosure

To date the worst breach in U.S. history. Court Ventures sold information directly to a Vietnamese fraudster (since arrested). The sale involved as many as 200 million American citizens' records, including Social Security numbers and financial data, which were offered by the fraudster to unscrupulous buyers through the site SuperGet.info.

Records breached **200m** No. of criminals with access to the data **1,300+**

Target Corp.

Method: Hack Attacker: At large

Records breached **40m** 4th qtr fall in profits **46%**

The Home Depot

Method: Hack Attackers: Two suspects in Detroit custody

In September 2014 it was revealed that a significant data breach had compromised the information of 56m Home Depot customers. The breach included credit and debit card information as well as names and addresses of the consumers affected.

Records breached **56m** No. of lawsuits filed against Home Depot **21**

Total records breached since 2005	Median avg. no. of records across all data breaches	Year since '05 with most breaches over 50k records	Sector with most records breached since 2005
930m	**2,300**	**2006**	**Financial**

Data source: Privacy Rights Clearinghouse

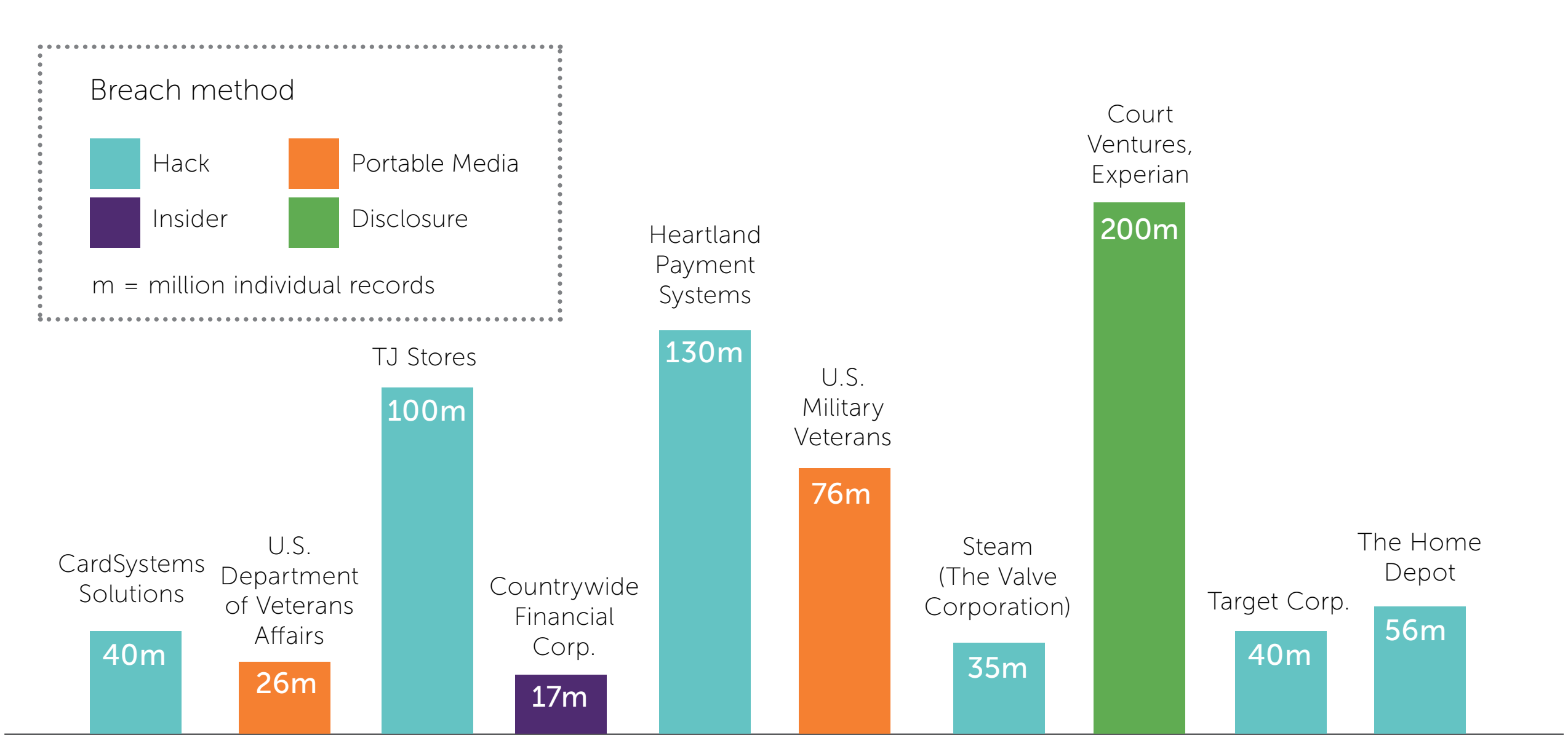
By total records breached, Business-Financial and Business-Retail are the worst affected sectors, with about half a billion records between them. One breach in particular contributed 200 million records to that total. It is, as of October 2014, the biggest compromise of data in U.S. history, involving sensitive personal information belonging to 2 out of 3 American citizens.

In brief, here's what happened. A data brokering company called Court Ventures, in conjunction with another company called U.S. Info Search, granted access to their database of millions of Americans' personal information (including social security numbers, addresses and phone numbers) to a Vietnamese national called Hieu Minh Ngo, who posed as a private investigator to get past their screening process. Over the next 18 months, Ngo had access to some 200 million records and, through his ID theft business superget.info, made at least $1.9 million selling millions of those records to more than 1,300 customers.

Court Ventures is now owned by another large data broker, Experian, who have tried quite hard to downplay their involvement in the whole debacle, probably in part because it was avoidable: the Secret Service told the CEO of U.S. Info Search that Ngo, the man illegally selling the data, had paid Experian his monthly data access charges with wire transfers sent from Singapore.

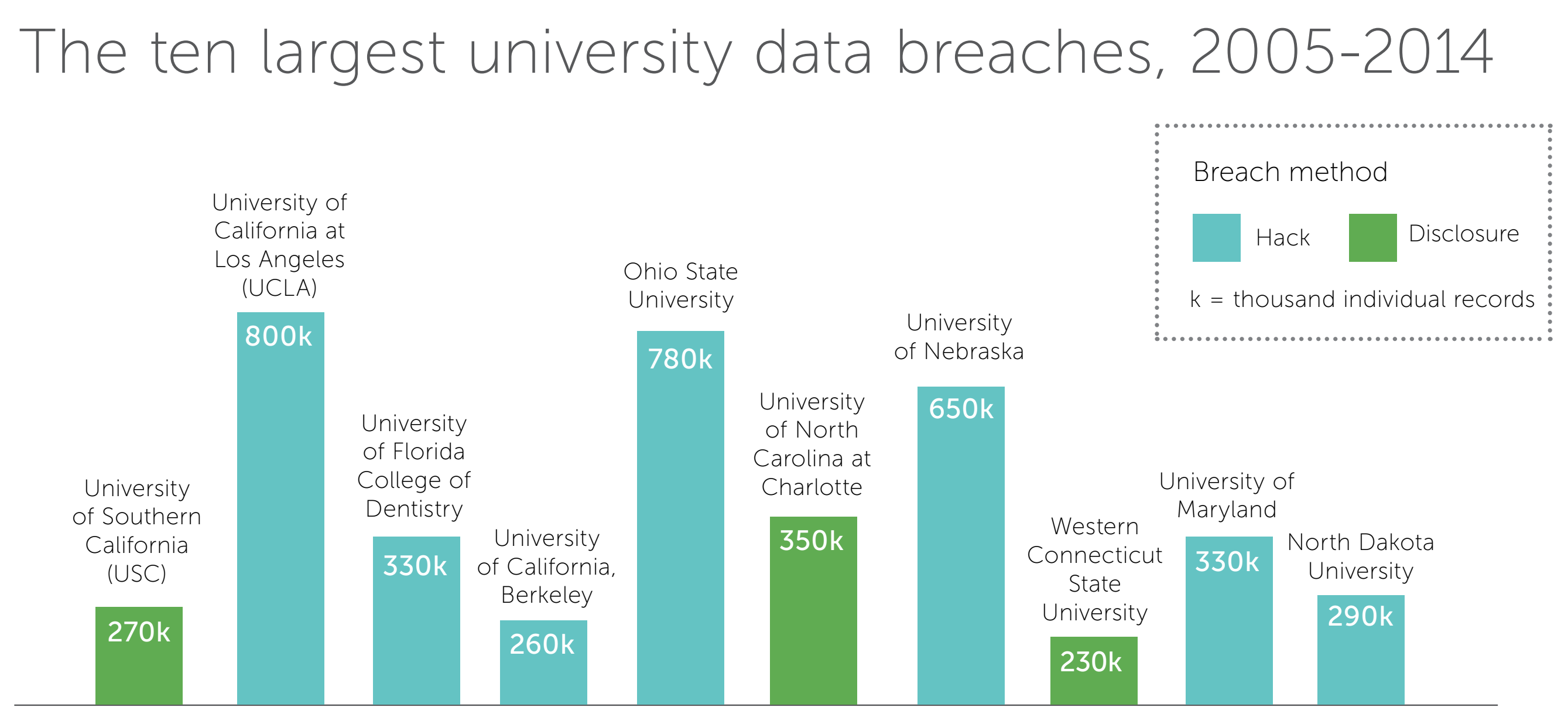
In fact, most of the data breaches on the chart above were similarly avoidable. Verizon, in their 2012 data breach report, calculated that 97% of breaches in that year could have been prevented. This is the crux of the litigation against these companies; maybe none of this had to happen.

The ten largest data breaches, 2005-2014



Six of the top ten data breaches since 2005 were hacks and, interestingly, every data breach of over 50,000 records this year (as of Oct. 28th 2014) have been hacks as well. This is mostly due to breaches of networks belonging to major retailers like Target (40m) and TJ Maxx (100m), as well as the Heartbleed security hole, which increased the prevalence of online spying and theft. But it's not just big businesses who fall prey to hackers with a hunger for big data. Educational institutions have been hit, too.

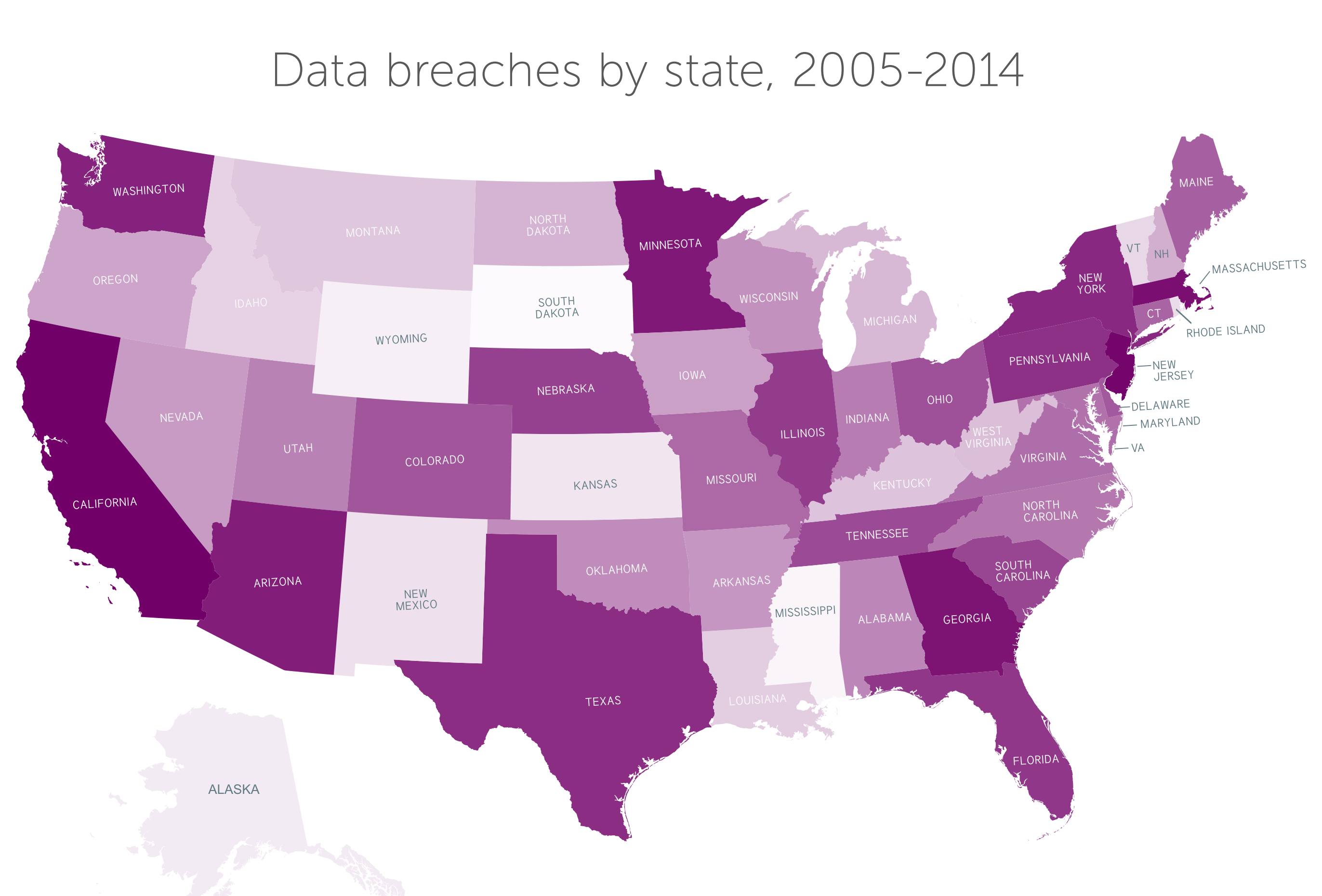
The ten largest university data breaches, 2005-2014



The largest breach of university data was at UCLA and, unsurpisingly, it was a hack. Up to 800,000 records were stolen, containing personal information on students (former and current), faculty members, and even people who didn't attend the university. Types of info included names, social security numbers and dates of birth.

Here is how all data breaches since 2005 are distributed across the United States. The following maps rank the 50 states by the total number of records that have been compromised within their borders.

Data breaches by state, 2005-2014

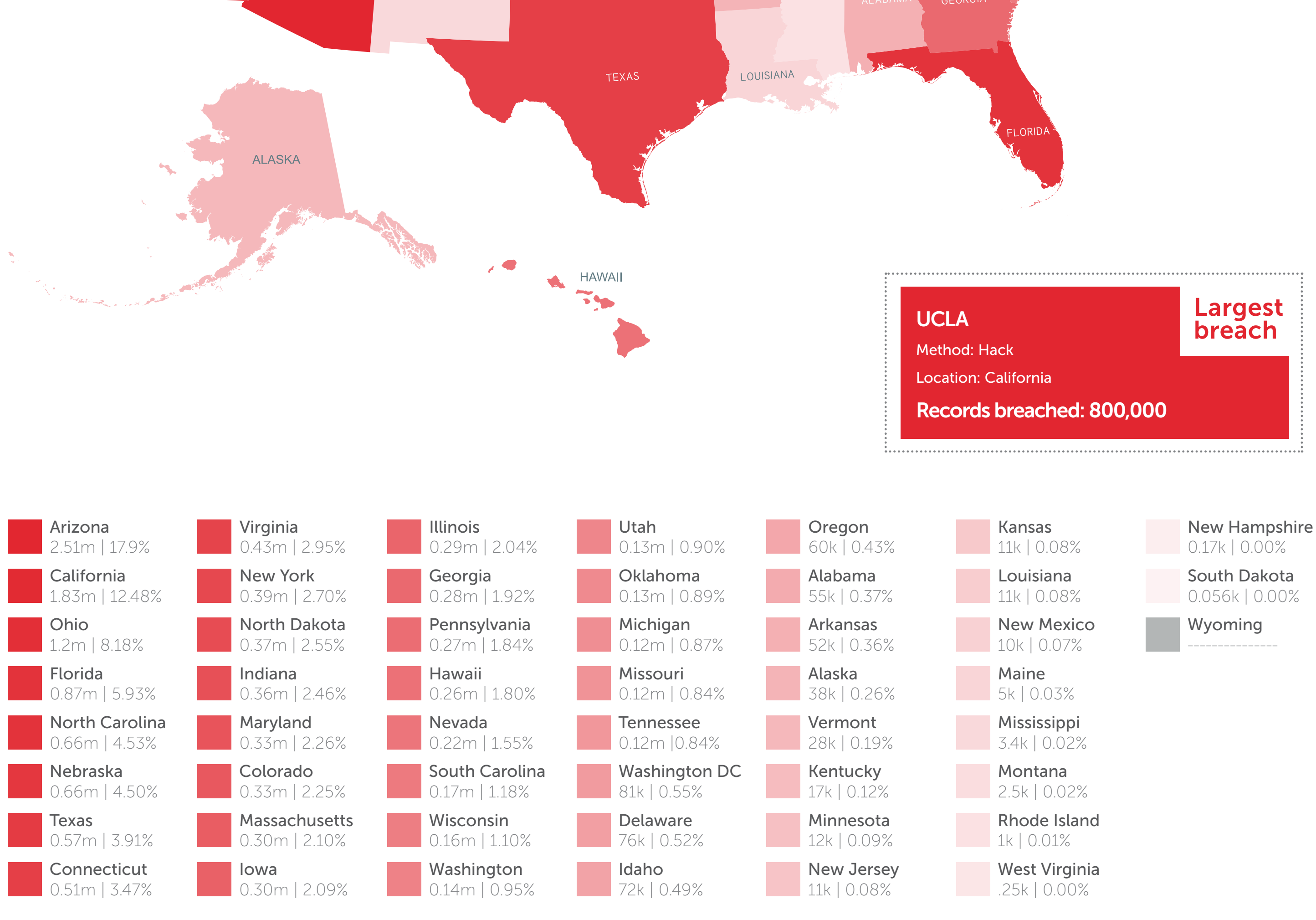

WASHINGTON
OREGON
CALIFORNIA
NEVADA
IDAHO
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
SOUTH CAROLINA
NORTH CAROLINA
VIRGINIA
WEST VIRGINIA
PENNSYLVANIA
NEW YORK
VT
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA
ALASKA
HAWAII

Court Ventures
Method: Disclosure
Location: Anaheim, California
Records breached: 200 million
Largest breach

California	233m	25.09%
New Jersey	132m	14.24%
Washington DC	104m	11.23%
Massachusetts	102m	10.96%
Georgia	75m	8.12%
Minnesota	44m	4.77%
Arizona	42m	4.61%
Washington	36m	3.88%
New York	27m	2.93%
Texas	19m	2.15%
Pennsylvania	15m	1.62%
Florida	14m	1.53%
Illinois	9.5m	1.02%
Nebraska	7.6m	0.83%
South Carolina	7.1m	0.77%
Tennessee	6m	0.65%
Ohio	6m	0.64%
Colorado	4.8m	0.54%
Delaware	4.2m	0.46%
Maine	4.2m	0.45%
Connecticut	3.2m	0.35%
Missouri	2.8m	0.30%
Virginia	25m	0.27%
Maryland	25m	0.25%
North Carolina	2.2m	0.25%
Indiana	1.8m	0.20%
Utah	1.7m	0.19%
Alabama	1.6m	0.18%
Oklahoma	1.6m	0.18%
Wisconsin	1.1m	0.11%
Arkansas	0.9m	0.10%
Nevada	0.6m	0.07%
Iowa	0.6m	0.07%
Oregon	0.5m	0.06%
Hawaii	0.4m	0.05%
New Hampshire	0.3m	0.04%
North Dakota	0.3m	0.04%
Michigan	0.3m	0.04%
West Virginia	0.2m	0.03%
Kentucky	0.2m	0.03%
Montana	0.2m	0.03%
Louisiana	0.1m	0.02%
Idaho	0.1m	0.01%
Vermont	0.1m	0.01%
Rhode Island	0.1m	0.01%
New Mexico	0.06m	0.01%
Kansas	0.05m	0.01%
Alaska	0.04m	0.00%
Wyoming	0.01m	0.00%
Mississippi	0.01m	0.00%
South Dakota	0.01m	0.00%

Court Ventures, with 200 million records, pushes California to the top of the state rankings table. Separating the breaches by sector reveals more. We'll start with Education.

Data breaches in the Education sector by state, 2005-2014

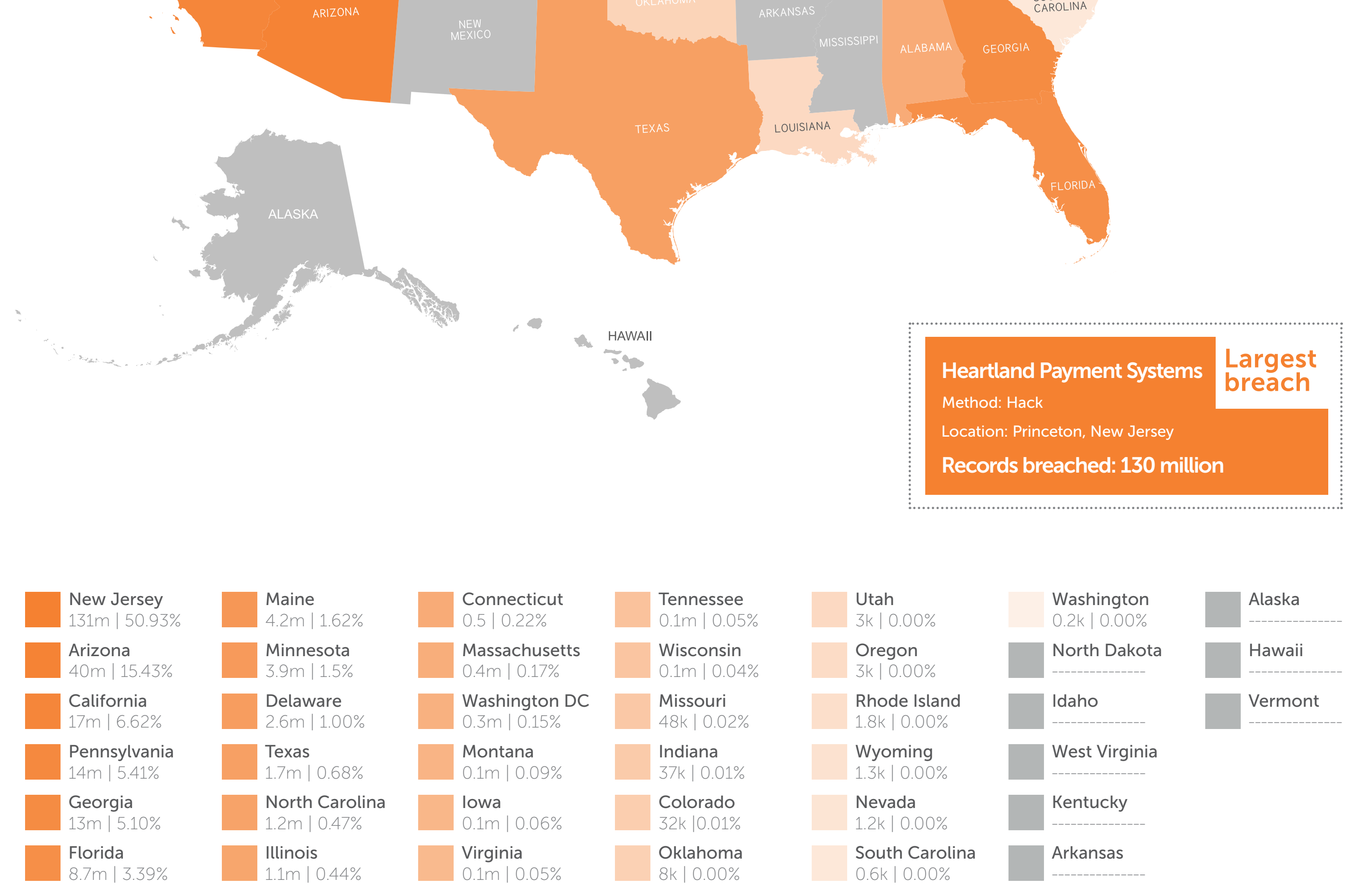

WASHINGTON
OREGON
CALIFORNIA
NEVADA
IDAHO
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
SOUTH CAROLINA
NORTH CAROLINA
VIRGINIA
WEST VIRGINIA
PENNSYLVANIA
NEW YORK
VT
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA
ALASKA
HAWAII

UCLA
Method: Hack
Location: California
Records breached: 800,000
Largest breach

Arizona	2.51m	17.9%
California	1.83m	12.48%
Ohio	1.2m	8.18%
Florida	0.87m	5.93%
North Carolina	0.66m	4.53%
Nebraska	0.66m	4.50%
Texas	0.57m	3.91%
Connecticut	0.51m	3.47%
Virginia	0.43m	2.95%
New York	0.39m	2.70%
North Dakota	0.37m	2.55%
Indiana	0.36m	2.46%
Maryland	0.33m	2.26%
Colorado	0.33m	2.25%
Massachusetts	0.30m	2.10%
Iowa	0.30m	2.09%
Illinois	0.29m	2.04%
Georgia	0.28m	1.92%
Pennsylvania	0.27m	1.84%
Hawaii	0.26m	1.80%
Nevada	0.22m	1.55%
South Carolina	0.17m	1.18%
Wisconsin	0.16m	1.10%
Washington	0.14m	0.95%
Utah	0.13m	0.90%
Oklahoma	0.13m	0.89%
Michigan	0.12m	0.87%
Missouri	0.12m	0.84%
Tennessee	0.12m	0.84%
Washington DC	81k	0.55%
Delaware	76k	0.52%
Idaho	72k	0.49%
Oregon	60k	0.43%
Alabama	55k	0.37%
Arkansas	52k	0.36%
Alaska	38k	0.26%
Vermont	28k	0.19%
Kentucky	17k	0.12%
Minnesota	12k	0.09%
New Jersey	11k	0.08%
Kansas	11k	0.08%
Louisiana	11k	0.08%
New Mexico	10k	0.07%
Maine	5k	0.03%
Mississippi	3.4k	0.02%
Montana	2.5k	0.02%
Rhode Island	1k	0.01%
West Virginia	.25k	0.00%
New Hampshire	0.17k	0.00%
South Dakota	0.056k	0.00%
Wyoming		

Despite UCLA having the single largest breach since 2005, California doesn't rank number one overall—Arizona does. That's thanks to an entity most people won't even have heard of: Maricopa County Community College District. Their security breach in 2013 exposed the personal information of 2.4 million people. In May 2014, a class action lawsuit was filed against them by two students, who sought $2,500 each in compensation.

Data breaches in the Financial & Insurance sector by state, 2005-2014

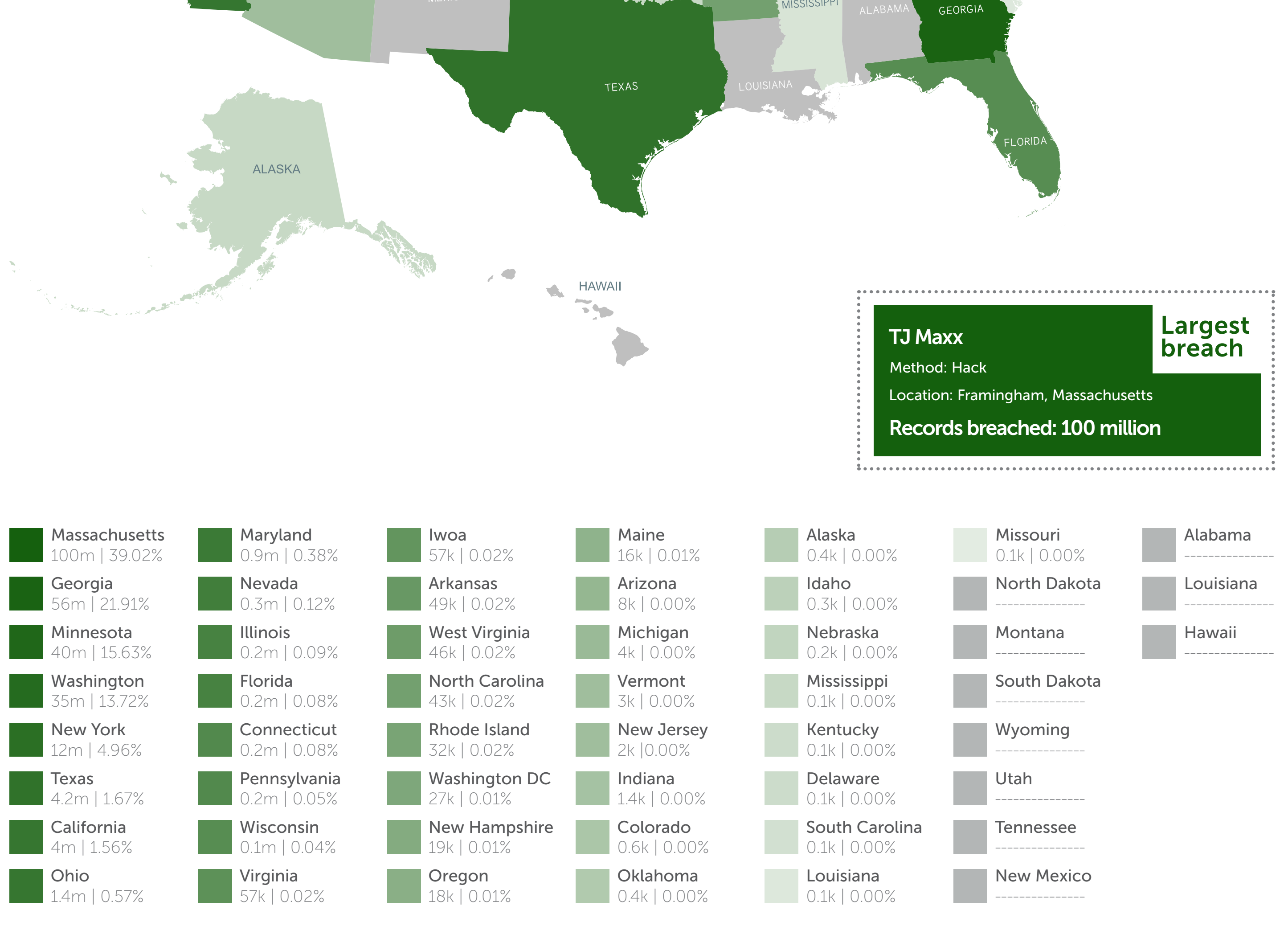

WASHINGTON
OREGON
CALIFORNIA
NEVADA
IDAHO
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
SOUTH CAROLINA
NORTH CAROLINA
VIRGINIA
WEST VIRGINIA
PENNSYLVANIA
NEW YORK
VT
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA
ALASKA
HAWAII

Heartland Payment Systems
Method: Hack
Location: Princeton, New Jersey
Records breached: 130 million
Largest breach

New Jersey	131m	50.93%
Arizona	40m	15.43%
California	17m	6.62%
Pennsylvania	14m	5.41%
Georgia	13m	5.10%
Florida	8.7m	3.39%
New York	8m	3.12%
Nebraska	6.5m	2.51%
Maine	4.2m	1.62%
Minnesota	3.9m	1.5%
Delaware	2.6m	1.00%
Texas	1.7m	0.68%
North Carolina	1.2m	0.47%
Illinois	1.1m	0.44%
Ohio	1m	0.40%
Alabama	1m	0.40%
Connecticut	0.5	0.22%
Massachusetts	0.4m	0.17%
Washington DC	0.3m	0.15%
Montana	0.1m	0.09%
Iowa	0.1m	0.06%
Virginia	0.1m	0.05%
Maryland	0.1m	0.05%
New Hampshire	0.1m	0.05%
Tennessee	0.1m	0.05%
Wisconsin	0.1m	0.04%
Missouri	48k	0.02%
Indiana	37k	0.01%
Colorado	32k	0.01%
Oklahoma	8k	0.00%
Michigan	6k	0.00%
Louisiana	4k	0.00%
Utah	3k	0.00%
Oregon	3k	0.00%
Rhode Island	1.8k	0.00%
Wyoming	1.3k	0.00%
Nevada	1.2k	0.00%
South Carolina	0.6k	0.00%
South Dakota	0.4k	0.00%
Kansas	0.2k	0.00%
Washington	0.2k	0.00%
North Dakota		
Idaho		
West Virginia		
Kentucky		
Arkansas		
Mississippi		
New Mexico		
Alaska		
Hawaii		
Vermont		

New Jersey is currently in first position for total records breached in the Financial and Insurance sector, thanks to the hack of Heartland Payment Systems in 2009, which may have been the result of a global cyber fraud operation. As of April 2012, the total sum of money awarded to victims of the breach was $1,925. Despite the breach affecting 130 million people and the settlement notice reaching at least 81.4% of them, only 11 valid claims were submitted and processed. Educating the people on their rights and entitlements with regard to class action settlements is part of our mission at the firm. Additionally, sites like this (that list class action settlements) can be a useful tool for consumers.

Data breaches in the Retail sector by state, 2005-2014

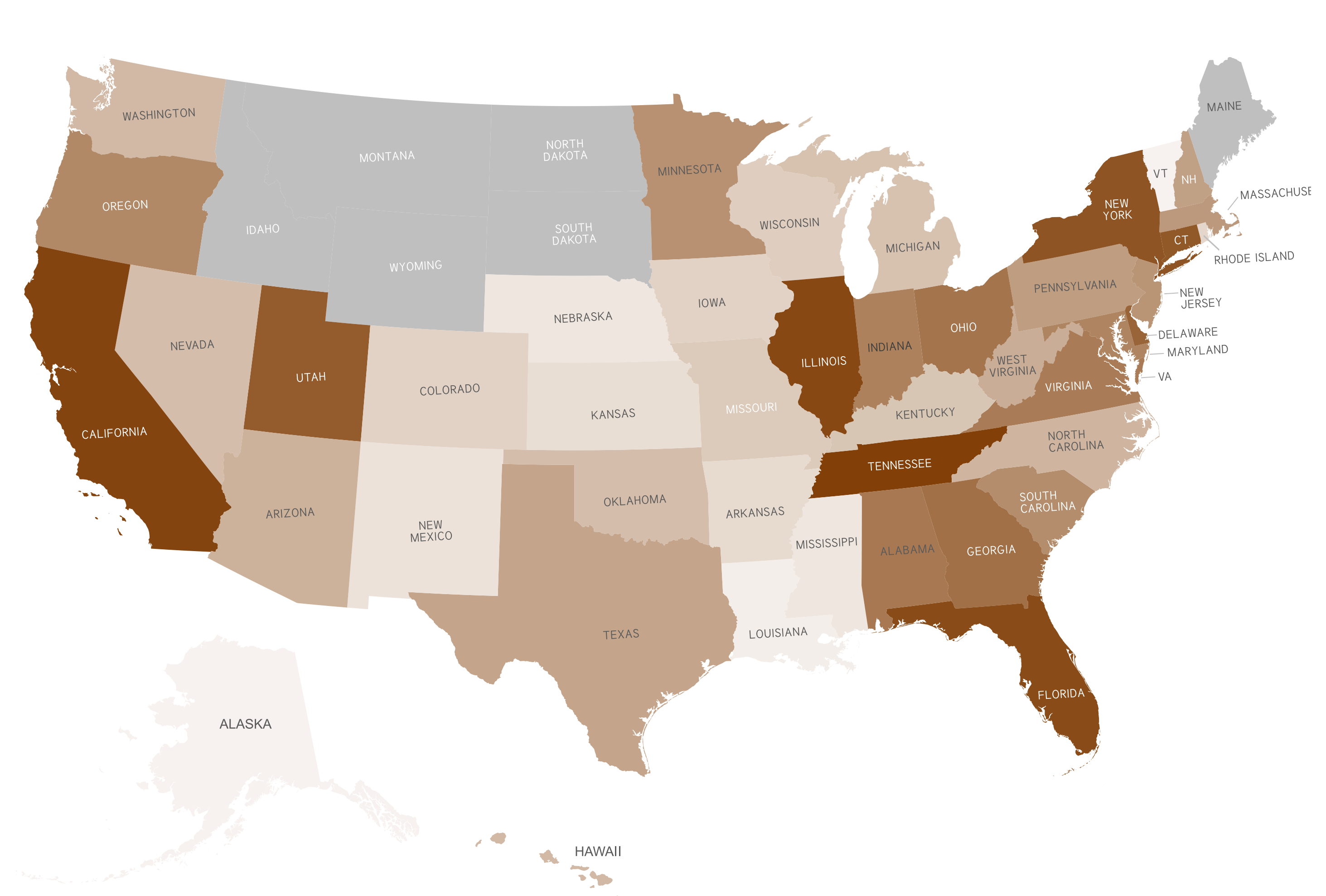

WASHINGTON
OREGON
CALIFORNIA
NEVADA
IDAHO
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
SOUTH CAROLINA
NORTH CAROLINA
VIRGINIA
WEST VIRGINIA
PENNSYLVANIA
NEW YORK
VT
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA
ALASKA
HAWAII

TJ Maxx
Method: Hack
Location: Framingham, Massachusetts
Records breached: 100 million
Largest breach

Massachusetts	100m	39.02%
Georgia	56m	21.91%
Minnesota	40m	15.63%
Washington	35m	13.72%
New York	12m	4.96%
Texas	4.2m	1.67%
California	4m	1.56%
Ohio	1.4m	0.57%
Maryland	0.9m	0.38%
Nevada	0.3m	0.12%
Illinois	0.2m	0.09%
Florida	0.2m	0.08%
Connecticut	0.2m	0.08%
Pennsylvania	0.2m	0.05%
Wisconsin	0.1m	0.04%
Virginia	57k	0.02%
Iwoa	57k	0.02%
Arkansas	49k	0.02%
West Virginia	46k	0.02%
North Carolina	43k	0.02%
Rhode Island	32k	0.02%
Washington DC	27k	0.01%
New Hampshire	19k	0.01%
Oregon	18k	0.01%
Maine	16k	0.01%
Arizona	8k	0.00%
Michigan	4k	0.00%
Vermont	3k	0.00%
New Jersey	2k	0.00%
Indiana	1.4k	0.00%
Colorado	0.6k	0.00%
Oklahoma	0.4k	0.00%
Alaska	0.4k	0.00%
Idaho	0.3k	0.00%
Nebraska	0.2k	0.00%
Mississippi	0.1k	0.00%
Kentucky	0.1k	0.00%
Delaware	0.1k	0.00%
South Carolina	0.1k	0.00%
Louisiana	0.1k	0.00%
Missouri	0.1k	0.00%
North Dakota		
Montana		
South Dakota		
Wyoming		
Utah		
Tennessee		
New Mexico		
Alabama		
Louisiana		
Hawaii		

There has been a slew of retail chain data breaches since late 2013, mostly involving credit and debit card fraud. In January 2014, Target announced a breach affecting 70 million customers, but that still didn't put them, and the state their headquarters reside in, at the top of the rankings above. That dubious accolade belongs to TJ Maxx, based in Massachusetts, who suffered a breach of about 100 million records in 2007. However, the event—which at the time was the largest ever data breach—didn't end up hurting the company too much. Much like Adobe Systems and JP Morgan, who have both experienced their own multi-million record breaches, TJ Maxx went on to see its stocks soar to five times their pre-breach levels.

Data breaches in the Medical sector by state, 2005-2014

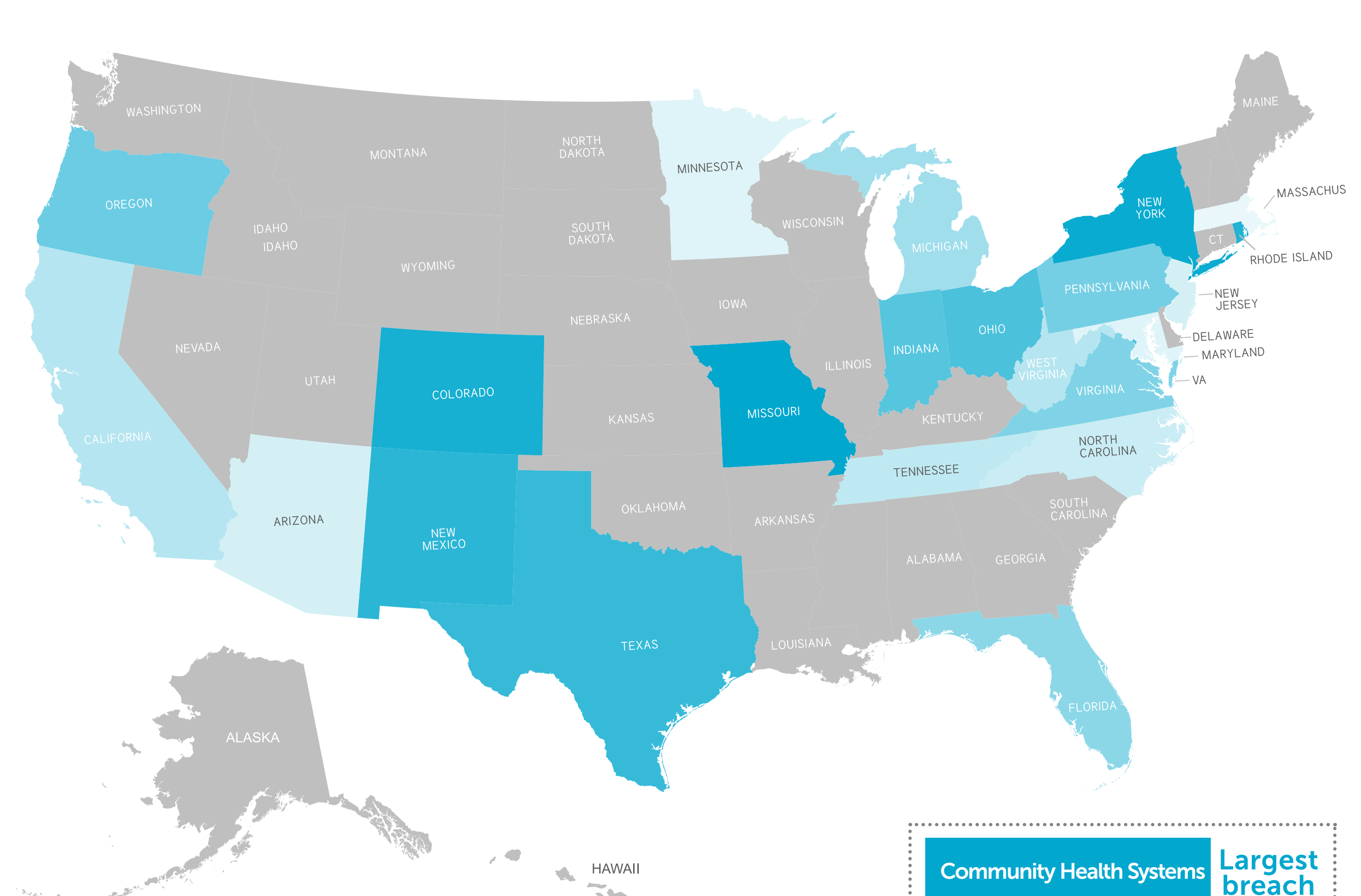

WASHINGTON
OREGON
CALIFORNIA
IDAHO
NEVADA
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
ALASKA
HAWAII
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
OHIO
WEST VIRGINIA
VIRGINIA
NORTH CAROLINA
SOUTH CAROLINA
PENNSYLVANIA
NEW YORK
VT
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA

Community Health Systems **Largest breach**
Method: Hack
Location: Franklin, Tennessee
Records breached: 4.5m

■ Tennessee 5.4m | 15.93%
■ California 4.8m | 14.36%
■ Illinois 4.5m | 13.24%
■ Florida 3.7m | 11.04%
■ New York 2.5m | 7.60%
■ Connecticut 1.7m | 5.03%
■ Delaware 1.6m | 4.69%
■ Utah 1.3m | 3.84%
■ Georgia 1.1m | 3.30%
■ Ohio 0.8m | 2.52%
■ Alabama 0.5m | 1.74%
■ Virginia 0.5m | 1.74%
■ Indiana 0.5m | 1.50%
■ Maryland 0.4m | 1.37%
■ Oregon 0.4m | 1.29%
■ South Carolina 0.4m | 1.22%
■ Minnesota 0.3m | 1.14%
■ New Jersey 0.3m | 0.88%
■ Massachusetts 0.28m | 0.84%
■ Pennsylvania 0.25m | 0.74%
■ New Hampshire 0.24m | 0.71%
■ Texas 0.23m | 0.70%
■ West Virginia 0.21m | 0.63%
■ Arizona 0.2m | 0.61%
■ North Carolina 0.18m | 0.55%
■ Washington 0.17m | 0.50%
■ Hawaii 0.13m | 0.38%
■ Nevada 0.12m | 0.38%
■ Oklahoma 0.1m | 0.31%
■ Michigan 98k | 0.29%
■ Washington DC 90k | 0.27%
■ Kentucky 75k | 0.22%
■ Missouri 39k | 0.12%
■ Wisconsin 20k | 0.06%
■ Iowa 19k | 0.06%
■ Colorado 15k | 0.05%
■ Rhode Island 14k | 0.04%
■ Arkansas 12k | 0.04%
■ Kansas 12k | 0.04%
■ New Mexico 4k | 0.04%
■ Nebraska 3k | 0.01%
■ Mississippi 2k | 0.01%
■ Louisiana 2k | 0.01%
■ Alaska 0.8k | 0.00%
■ Vermont 0.1k | 0.00%
■ Maine
■ Montana
■ Idaho
■ South Daktota
■ North Dakota
■ Wyoming

It's believed that Chinese hackers were responsible for the data breach earlier this year of 4.5 million records held by Community Health Systems in Tennessee (putting the state in first place, just ahead of California). Five Alabama residents have filed a class action lawsuit as a result of the breach.

Non-profit breaches by state, 2005-2014

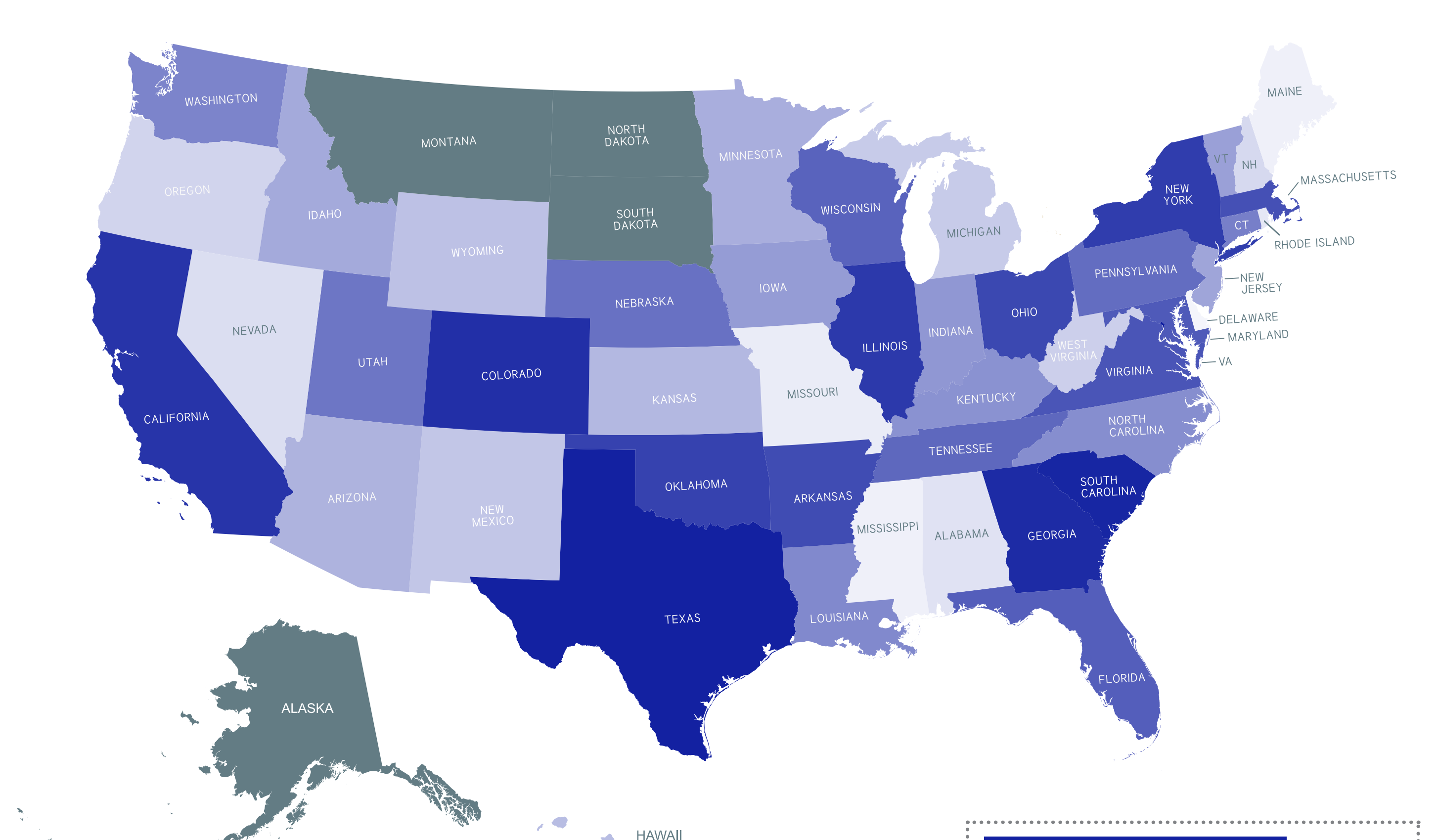

WASHINGTON
OREGON
CALIFORNIA
IDAHO
NEVADA
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
ALASKA
HAWAII
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
OHIO
WEST VIRGINIA
VIRGINIA
NORTH CAROLINA
SOUTH CAROLINA
PENNSYLVANIA
NEW YORK
VT
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA

Community Health Systems **Largest breach**
Method: Hack
Location: Franklin, Tennessee
Records breached: 4.5m

■ Missouri 1.0m | 52.19%
■ New York 0.4m | 22.99%
■ Colorado 0.2m | 9.87%
■ Rhode Island 70k | 3.46%
■ New Mexico 36k | 1.78%
■ Texas 35k | 1.73%
■ Washington DC 28k | 1.39%
■ Ohio 26k | 1.31%
■ Indiana 19k | 0.95%
■ Oregon 19k | 0.94%
■ Pennsylvania 15k | 0.74%
■ Virginia 14k | 0.74%
■ Florida 12k | 0.60%
■ Michigan 10k | 0.50%
■ California 9.7k | 0.48%
■ West Virginia 2.5k | 0.12%
■ Tennessee 1.5k | 0.08%
■ North Carolina 1.3k | 0.07%
■ New Jersey 0.8km | 0.04%
■ Maryland 0.2k | 0.01%
■ Massachusetts 0.2k | 0.01%
■ Arizona 0.1k | 0.01%
■ Minnesota 0.04k | 0.00%
■ Washington
■ Montana
■ North Dakota
■ Wisconsin
■ Vermont
■ New Hampshire
■ Maine
■ Connecticut
■ Delaware
■ Kentucky
■ Illinois
■ Iowa
■ Nebraska
■ South Dakota
■ Kansas
■ Wyoming
■ Utah
■ Nevada
■ Oklahoma
■ Arkansas
■ Louisiana
■ Mississippi
■ Alabama
■ Gerogia
■ South Carolina
■ Hawaii
■ Alaska
■ Idaho

Non-profit organizations have survived relatively unscathed since 2005, with Missouri, in first place, losing 'only' 1 million records in data breaches in the last nine years. The 1 million records that *were* compromised in Missouri were accessed by a dishonest employee of the St. Louis chapter of the Red Cross, who used the information of at least three of the one million people affected to commit identity theft.

Government & Military data breaches by state, 2005-2014


WASHINGTON
OREGON
CALIFORNIA
IDAHO
NEVADA
MONTANA
WYOMING
UTAH
ARIZONA
COLORADO
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
OKLAHOMA
TEXAS
ALASKA
HAWAII
MINNESOTA
IOWA
MISSOURI
ARKANSAS
LOUISIANA
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
KENTUCKY
TENNESSEE
MISSISSIPPI
ALABAMA
GEORGIA
FLORIDA
OHIO
WEST VIRGINIA
VIRGINIA
NORTH CAROLINA
SOUTH CAROLINA
PENNSYLVANIA
NEW YORK
NH
MAINE
MASSACHUSETTS
CT
RHODE ISLAND
NEW JERSEY
DELAWARE
MARYLAND
VA

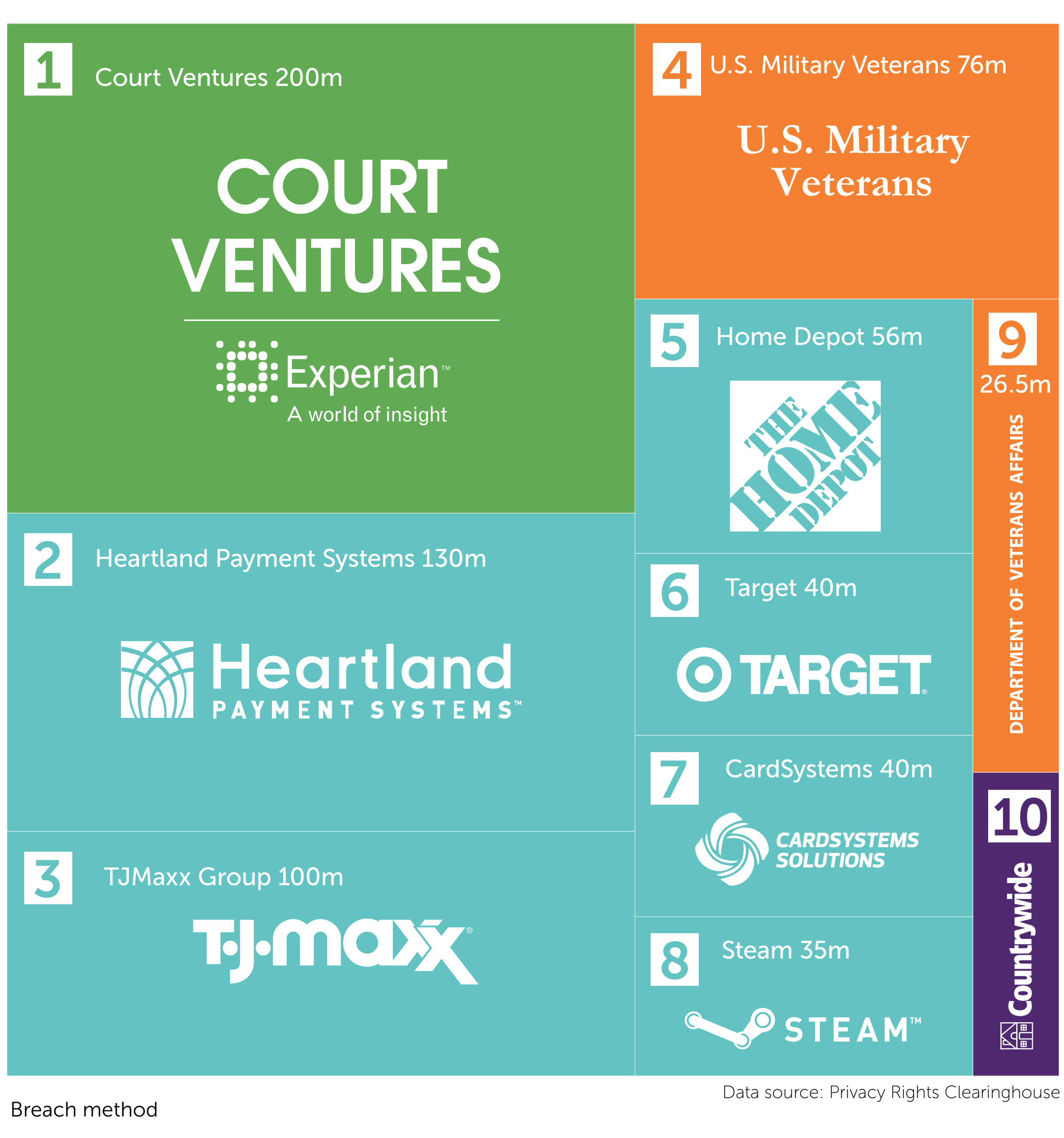
U.S. Military Veterans **Largest breach**
Method: Portable Media
Location: Washington DC
Records breached: 76 million

■ Washington DC 103m | 69.89%
■ Texas 11m | 7.95%
■ South Carolina 6.4m | 4.34%
■ Georgia 4.4m | 3.3%
■ Colorado 4.3m | 2.95%
■ California 3.9m | 2.63%
■ Illinois 3m | 2.07%
■ New York 1.4m | 0.97%
■ Oklahoma 1.3m | 0.93%
■ Ohio 1m | 0.70%
■ Arkansas 0.8m | 0.57%
■ Massachusetts 0.7m | 0.50%
■ Virginia 0.6m | 0.43%
■ Maryland 0.6m | 0.42%
■ Florida 0.55m | 0.37%
■ Wisconsin 0.54m | 0.37%
■ Tennessee 0.3m | 0.24%
■ Pennsylvania 0.3m | 0.22%
■ Nebraska 0.3m | 0.21%
■ Utah 0.3m | 0.20%
■ Connecticut 0.18m | 0.12%
■ Washington 0.18m | 0.12%
■ Louisiana 0.16m | 0.11%
■ North Carolina 0.15m | 0.10%
■ Kentucky 0.14m | 0.10%
■ Indiana 0.1m | 0.07%
■ Iowa 94k | 0.06%
■ Vermont 71k | 0.05%
■ New Jersey 68k | 0.05%
■ Idaho 62k | 0.04%
■ Minnesota 52k | 0.04%
■ Arizona 42k | 0.03%
■ Kansas 29k | 0.02%
■ Hawaii 16k | 0.01%
■ Wyoming 14k | 0.01%
■ New Mexico 12k | 0.01%
■ Michigan 12k | 0.01%
■ West Virginia 11k | 0.01%
■ Oregon 10k | 0.01%
■ Nevada 9k | 0.01%
■ Alabama 8k | 0.01%
■ Rhode Island 8k | 0.01%
■ Mississippi 8k | 0.01%
■ Missouri 5k | 0.00%
■ Maine 0.1k | 0.00%
■ Delaware 0.1k | 0.00%
■ Montana
■ North Dakota
■ South Dakota
■ Alaska
■ Wyoming

The state, so to speak, at the top of the list for Government and Military data breaches is, as you might have guessed, Washington DC. The agency responsible for most of the compromised records is U.S. Military Veterans, who in 2009 sent a defective hard drive containing a very large Oracle database back to its vendor to be fixed. The vendor determined it could not be repaired and sent it to another firm for recycling. Along the way, 76 million records from the Oracle database on the drive were exposed.

Here is a final visual summary of the top 25 largest data breaches since 2005.

Top 10 data breaches by total records compromised, 2005-2014

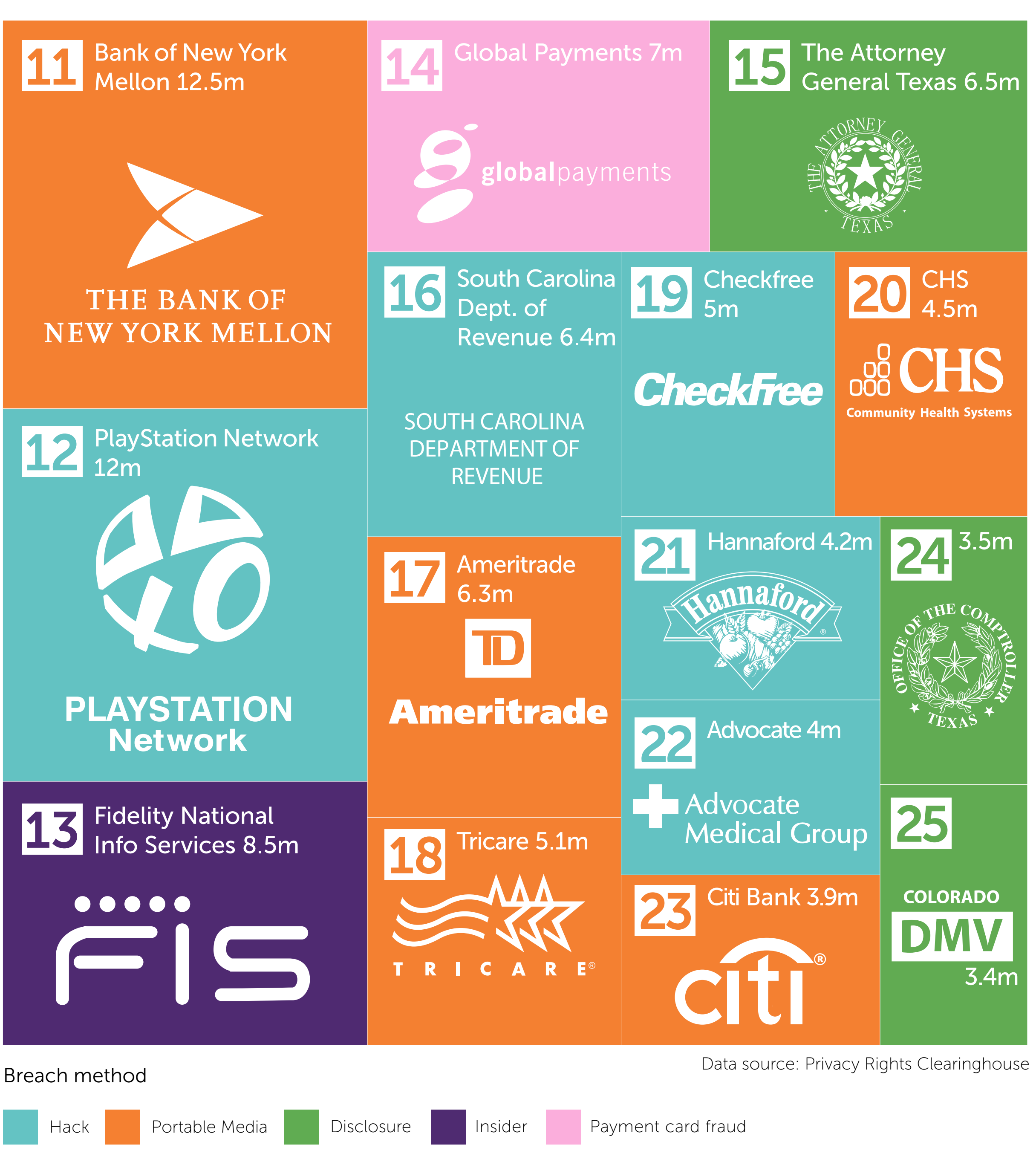


Data source: Privacy Rights Clearinghouse

Breach method

🟦 Hack 🟧 Portable Media 🟩 Disclosure 🟪 Insider

Top 11-25 data breaches by total records compromised, 2005-2014



Data source: Privacy Rights Clearinghouse

Breach method

🟦 Hack 🟧 Portable Media 🟩 Disclosure 🟪 Insider 🟪 Payment card fraud

It's interesting to note that, even with a clear overview of all of the data breaches that have occurred in recent years, finding trends and patterns in how personal information is being compromised is extremely difficult. A couple of times a year, we see individual breaches on an epic scale (tens or hundreds of millions of records), while in the months between, there are dozens, if not hundreds, of smaller but still very substantial exposures of personal information, from all sectors and by all possible means.

President Obama recently (October 17th, 2014) announced a plan to introduce chip-and-PIN technology to new credit and debit cards issued by the federal government (a security feature that has been standard for years outside the US), but he could only urge private sector corporations like Mastercard to follow suit. It's possible that new industry breach standards, which come into effect in October 2015, will force the change, as they will shift the cost of liability onto any bank or retailer who has not invested in the new, more secure technology. Time will tell. Until then--and afterwards, for that matter--keep a close eye on your bank balance and credit score.

Assets

The graphics on this page can be downloaded via the following link. Please retain the attribution on the images and, if possible, link back to this page.

Download assets

Sources

All graphics on this page were made using data from Privacy Clearinghouse:
http://www.privacyrights.org/data-breach

http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/

http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/obama-calls-for-greater-credit-card-security-in-light-of-data-breaches/

http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf

http://www.foxbusiness.com/personal-finance/2014/07/23/study-data-breaches-pose-greater-risk/

http://www.usnews.com/news/articles/2014/05/28/companies-unprepared-as-hacking-increases

http://www.azcentral.com/story/news/local/phoenix/2014/05/02/lawsuit-filed-maricopa-districts-security-breach/8619189/

https://www.techdirt.com/articles/20120404/17441818377/final-stats-heartland-payment-systems-class-action-1925-to-11-people-600k-to-lawyers.shtml

http://www.forbes.com/sites/quickerbettertech/2014/06/02/why-did-t-j-maxxs-share-price-surge-after-a-data-breach-that-affected-94-million-customers/

http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf