BB2G

BORN BETWEEN 2 GENERALS

NATIONAL DATA RESILIENCE · 50 STATES + D.C.

Know where every record lives. Prove you can get it back.

Americans filed 1.1 million identity theft reports with the FTC in 2024 and lost a record $15.9 billion to fraud in 2025. The breaches on this map alone exposed more than 98 million health, tax, student, customer and driver records. This briefing maps the exposure in every state and shows how BB2G tracks sensitive data, keeps it on servers the state controls, and restores it on a clock.

BORN BETWEEN 2 GENERALS, LLC · NATIONAL DATA RESILIENCE

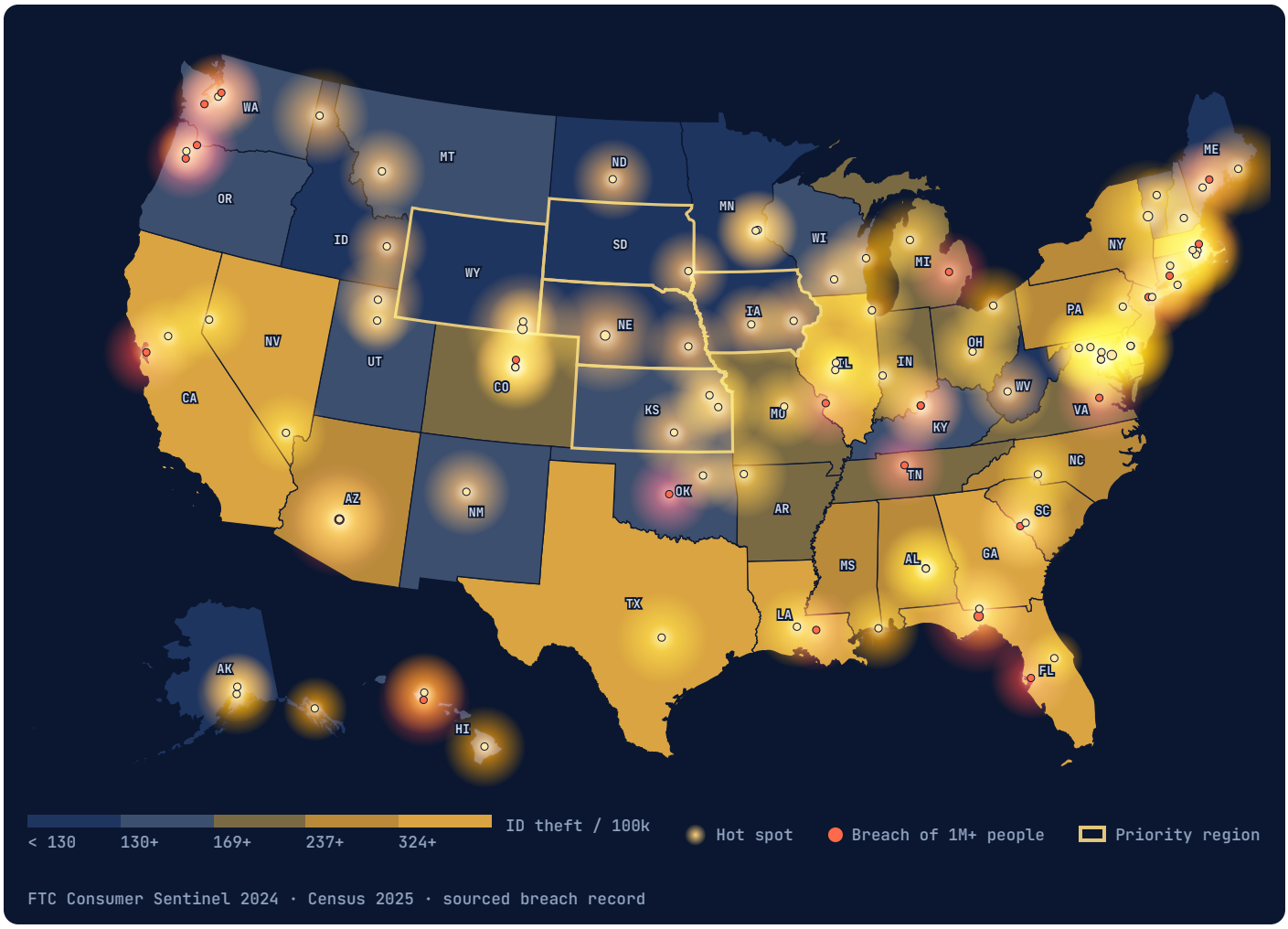
UPDATED NOV. 10, 2026

DATAMAP.BORNBETWEEN2GENERALS.COM

Where sensitive data is leaking

States are shaded by identity theft reports per 100,000 residents. Each glow is a documented breach of health, financial, student, government or driver records; red marks breaches of a million people or more.

1,135,291	$15.9B	97	99M+
Identity theft reports to the FTC in 2024	Fraud losses reported to the FTC in 2025, a record	Breaches documented across 51 jurisdictions	Records exposed in the breaches on this map



The identity theft belt

Florida (528 reports per 100k), Georgia (517), D.C. (480), Nevada (466) and Texas (393) report the most identity theft per resident.

Health data is the target

Hospitals and insurers dominate the record: Kaiser (13.4M), HCA (11M), Ascension (5.6M) and Yale New Haven (5.5M) in four years.

The priority region

Nebraska, Iowa, South Dakota, Kansas and Wyoming residents reported $192 million in fraud losses in 2024, and Change Healthcare reached 575,000 Nebraskans.

LATEST · JULY – NOV. 2026

What leaked this year

Recent breaches of sensitive public and health records, newest first.

A million people or more

NEW Oct 2026 · Florida

Florida student aid website breach may affect 4.9 million people

FLDOE announced unauthorized criminal access to the Florida Student Financial Aid website. Exposed data may include Social Security numbers, names, birth dates and addresses.

WWSB ABC7

NEW Sep 2026 · Phoenix, AZ

Arizona court system hack copies data on 1.3 million people

Attackers who got in through a phishing email copied court records on 1.3 million people, including unpaid fines and restitution going back 30 years. The records also include nearly 30,000 protection orders and about 150,000 foster care board reports.

KOLD News 13

Government, schools, courts and health

NEW Oct 2026 · Nebraska

North Platte and Lincoln County, Neb., knocked offline

A cyberattack on Oct. 9 knocked out internet and systems for the City of North Platte and Lincoln County. The governor declared an emergency and the Nebraska National Guard cyber team deployed; the mayor later said a stolen employee password caused the attack.

Government Technology

NEW Oct 2026 · Maryland

Anne Arundel County confirms breach as Rhysida demands $2 million

The county confirmed an unauthorized actor accessed a small number of systems in August and copied some files. The Rhysida ransomware gang claimed the attack, demanded $2 million and threatened to leak 2.6 TB of documents.

The Record

NEW Oct 2026 · Vermont

Slate Valley school district refuses ransom after data breach

Hackers accessed business documents and employee personal information in a September breach and demanded a ransom. On Oct. 2 the district said its board declined to pay on legal advice.

WCAX

NEW Sep 2026 · Wyoming

Court vendor breach exposes Wyoming court users' personal data

The Wyoming Judicial Branch said on Sept. 2, 2026, that court user data was obtained in a breach at its vendor, West Publishing Corporation, which also hit other court systems around the country. Names, addresses and dates of birth of people who dealt with district courts or the Supreme Court from 2015 to 2025 were compromised, and courts kept operating normally.

Wyoming Public Media

SENSITIVE DATA · NATIONAL DATA RESILIENCE + AUDIT NETWORK

Follow every record from birth to destruction

Health, tax, student, foster, voter, driver and court records pass through agencies, vendors, subcontractors, cloud hosts, processors and data brokers. BB2G maps each hop and holds every one to a legal basis.

1 Originate
Where the record was created and under what law: HIPAA, FERPA, DPPA, IRS 1075, CJIS or state statute.

2 Authorize
Who may hold it and why. No legal basis, no copy.

3 Store
Encrypted on servers the jurisdiction controls, with keys it holds.

4 Access
Named accounts, hardware keys and least privilege. Every read is logged.

5 Transfer
WAYBILL records each time data leaves: fields, recipient, basis, retention.

6 Retain and destroy
A retention clock on every record, verified deletion and a certificate of destruction.

THE SENSITIVE-DATA TOOLSET

WAYBILL
A custody slip for every outbound transfer of protected data, matched to a contract and a destruction date.

LINEAGE ATLAS
A map of where each data set came from and every system, vendor and subcontractor that touched it.

VENDOR AND BROKER MAP
Agencies, vendors, subcontractors, cloud hosts, processors and data brokers, with their contracts.

BREACH CLOCK
Each state's notification deadline starts the moment a breach is confirmed, with drafts ready.

MINIMUM NECESSARY
Share only the fields a task needs. No bulk files, no model training, no resale.

EVIDENCE GRADES
Every finding linked to its source and timestamp, separate from allegations.

THE SERVER STACK · SOVEREIGN HYBRID COMPUTE

Sensitive data stays on servers the state controls

Three planes, each with a hard boundary. Sensitive data never leaves the jurisdiction's own hardware; only signed, de-identified results move up.

PLANE 1 · SOVEREIGN

State and county servers

Air-gapped local servers inside the jurisdiction hold every sensitive record.

- Per-tenant isolation for each state and county
- Encryption keys held by the jurisdiction
- Write-once evidence vault
- No inbound internet path

PLANE 2 · WORKBENCH

ProBox local analysis

A local workbench runs analysis and AI on the loopback address with no outside connection.

- Runs on 127.0.0.1, zero egress
- Local AI models, no cloud prompts
- FIDO2 hardware keys to sign in
- Signed outputs only

PLANE 3 · CLOUD

Bounded cloud staging

Public dashboards and executive reports run in the cloud with no personal data at all.

- Aggregates and public records only
- Signed release receipts
- Security headers and audit logs
- Instant rollback

One-way, signed releases: data only moves up after it is de-identified, and every release gets a receipt

HARDENING ON EVERY SERVER

LATCHKEY

FIDO2 hardware keys for every administrator. No shared accounts, no SMS codes.

SPLIT-KEY CHANGES

Two separate hardware keys are required to change a security baseline or a backup target.

ZERO-TRUST ACCESS

Attribute-based access, mutual TLS between services and rate-limited tokens.

CREDENTIAL WATCH

Session tokens checked against breach dumps and code repositories; a match revokes them.

CUSTOMER-PRIVATE COMPUTE

Each customer's servers, identities and keys stay separate from BB2G's own.

WORKFORCE CONTROLS

Role-based training, assigned encrypted USB devices, offboarding and audit trails.

BACKSTOP · 3-2-1 RECOVERY

A backup isn't real until it's restored on a clock

Ransomware wins when backups are online, untested or encrypted along with everything else. BACKSTOP keeps copies the attacker can't reach and proves they work.

3	2	1
Copies of every critical data set	Different media: a live cluster and an air-gapped array	Encrypted copy off-site and offline

1 Write once
Backups land in write-once storage that no account, including an administrator, can alter or delete.

2 Hash every block
A Merkle hash tree fingerprints every backup so tampering shows instantly.

3 Isolate on breach
A confirmed breach triggers fresh mirrors and cuts the compromised network segment off.

4 Timed restore drill
Scheduled restores on synthetic data, timed against the recovery target.

5 Two-key reset
Returning to normal operations requires two hardware keys.

6 Receipt
Every drill and restore produces a signed receipt for auditors.

FAIL CLOSED If a backup's fingerprint doesn't match, it is never restored. The system stops, holds the last good copy and pages a named person.

WHY SMALL ERROR RATES BECOME BREACHES

A record crosses 20 hands. At 95% each, it's safe 36% of the time.

Every vendor, transfer, backup and access is a step where a record can be mishandled. Twenty steps at 95% each leaves a 64% chance something went wrong. Real data passes through far more than 20.

CHAIN LENGTH	95% PER STEP, NO CHECKS	99% PER STEP, NO CHECKS	95% PER STEP, BB2G CHECKS	99% PER STEP, BB2G CHECKS
10 steps	59.9%	90.4%	99.5%	99.90%
20 steps	35.8%	81.8%	99.0%	99.80%
50 steps	7.7%	60.5%	97.5%	99.50%
100 steps	0.6%	36.6%	95.1%	99.00%
200 steps	0.0%	13.4%	90.5%	98.02%

Chance the chain finishes with no undetected error. With BB2G, each step has a check that catches 99% of errors and stops the record instead of letting it move on.

A RECORD'S LIFE · GOLD STEPS ARE BB2G CHECKS

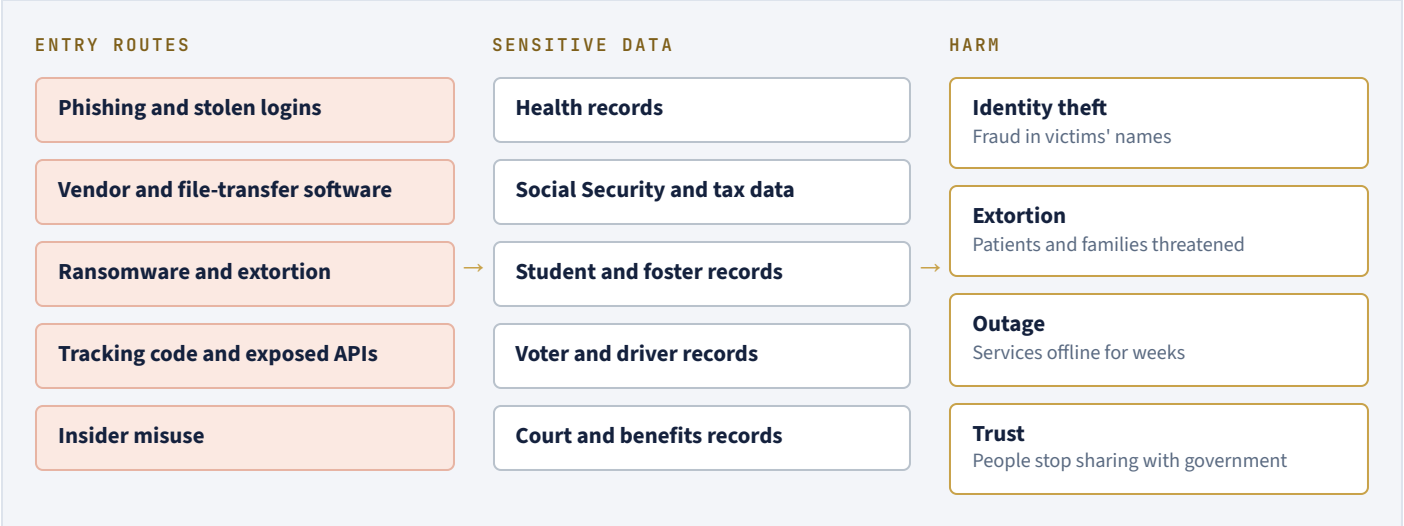
Collected · Classified · **Legal basis check** · Encrypted at rest · Indexed · Shared with vendor · **WAYBILL logged** · Subcontractor · Cloud processor · Analytics · Report · Backup · **Hash verified** · Restore drill · Access review · Retention clock · Incident watch · Breach notice · **Verified destruction** · Certificate

Knowing when to stop A check that finds a problem stops the record. Stopping is the feature: a paused record can be fixed; a leaked one can't be recalled.

EXPOSURE PATHWAY

Route to exposure, and where to break it

How sensitive records get out, and the controls that stop each route.



NATIONAL RANKINGS

How every state compares

Rank 1 has the most identity theft reports per 100,000 residents (FTC, 2024). Priority region shaded.

Rank	Jurisdiction	Region	ID theft / 100K	ID theft	Fraud / 100K	Fraud losses	Loss / resident	Breaches
1	**Florida**	South	528	115,840	2,163	$866.1M	$36.91	4
2	**Georgia**	South	517	55,955	2,108	$291.3M	$25.77	1
3	**District of Columbia**	South	480	3,225	2,509	$30.4M	$43.82	3
4	**Nevada**	West	466	14,631	1,867	$138.5M	$42.21	2
5	**Texas**	South	393	116,484	1,561	$897.9M	$28.32	1
6	**Delaware**	South	392	3,942	1,876	$34.3M	$32.34	2
7	**Massachusetts**	Northeast	388	27,141	1,165	$210.3M	$29.40	2
8	**California**	West	356	139,665	1,291	$1.68B	$42.66	2
9	**Louisiana**	South	346	15,991	1,472	$89.4M	$19.35	2
10	**Illinois**	Midwest	339	43,028	1,469	$318.1M	$25.01	3
11	**Maryland**	South	324	19,990	1,799	$198.9M	$31.75	2
12	**New Jersey**	Northeast	313	29,037	1,506	$314.4M	$32.93	1
13	**New York**	Northeast	295	58,692	1,402	$534.0M	$26.70	2
14	**South Carolina**	South	291	15,146	1,536	$137.0M	$24.60	1
15	**Pennsylvania**	Northeast	290	37,717	1,419	$285.4M	$21.85	1
16	**Arizona**	West	287	20,863	1,459	$336.7M	$44.17	2
17	**Alabama**	South	269	13,596	1,388	$104.2M	$20.07	2
18	**Mississippi**	South	268	7,903	1,221	$44.4M	$15.03	1
19	**Rhode Island**	Northeast	264	2,896	1,075	$20.7M	$18.53	2
20	**North Carolina**	South	259	27,466	1,369	$276.8M	$24.72	1
21	**Michigan**	Midwest	237	23,783	1,167	$204.0M	$20.15	2
22	**Connecticut**	Northeast	236	8,502	1,220	$90.3M	$24.50	2
23	**Ohio**	Midwest	236	27,766	1,115	$226.2M	$19.01	2
24	**Virginia**	South	213	18,460	1,361	$293.7M	$33.07	1
25	**Tennessee**	South	212	14,829	1,188	$157.2M	$21.49	1
26	**Arkansas**	South	209	6,340	971	$52.1M	$16.73	1
27	**Colorado**	West	208	12,087	1,260	$210.7M	$35.05	3
28	**Indiana**	Midwest	198	13,471	1,071	$112.3M	$16.10	1

RANK	JURISDICTION	REGION	ID THEFT / 100K	ID THEFT	FRAUD / 100K	FRAUD LOSSES	LOSS / RESIDENT	BREACHES
29	**Missouri**	Midwest	187	11,535	1,169	$139.3M	$22.22	2
30	**Oklahoma**	South	169	6,747	908	$72.7M	$17.64	2
31	**Washington**	West	169	13,068	1,134	$297.2M	$37.15	3
32	**Oregon**	West	163	6,898	1,090	$123.7M	$28.95	3
33	**Utah**	West	157	5,224	906	$113.1M	$31.96	2
34	**Kansas**	Midwest	154	4,518	848	$57.6M	$19.34	3
35	**New Mexico**	West	150	3,171	991	$56.6M	$26.63	1
36	**New Hampshire**	Northeast	150	2,079	1,033	$34.6M	$24.46	1
37	**Wisconsin**	Midwest	149	8,798	908	$106.0M	$17.75	2
38	**Kentucky**	South	142	6,396	859	$70.8M	$15.36	2
39	**Hawaii**	West	138	1,990	980	$61.6M	$42.99	3
40	**Montana**	West	131	1,447	873	$22.5M	$19.70	1
41	**Nebraska**	Midwest	130	2,554	887	$41.9M	$20.75	2
42	**Maine**	Northeast	127	1,746	879	$29.3M	$20.67	3
43	**Minnesota**	Midwest	127	7,280	906	$144.6M	$24.80	2
44	**Idaho**	West	125	2,367	849	$53.9M	$26.57	2
45	**Iowa**	Midwest	123	3,919	715	$52.0M	$16.04	2
46	**Wyoming**	West	120	697	899	$20.1M	$34.14	2
47	**North Dakota**	Midwest	119	924	696	$14.4M	$17.98	1
48	**West Virginia**	South	113	2,017	836	$27.0M	$15.30	2
49	**Alaska**	West	106	780	992	$26.9M	$36.54	3
50	**Vermont**	Northeast	101	651	908	$10.6M	$16.37	2
51	**South Dakota**	Midwest	94	845	676	$20.4M	$21.85	1

BREACH RECORD · 2016 – NOV. 2026

Sensitive data already exposed

Documented breaches of health, financial, student, government, court and voter records, newest first, each linked to its source.

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
2026			
Oct 2026	NEW **Nebraska** PRIORITY	**North Platte and Lincoln County, Neb., knocked offline** A cyberattack on Oct. 9 knocked out internet and systems for the City of North Platte and Lincoln County. The governor declared an emergency and the Nebraska National Guard cyber team deployed; the mayor later said a stolen employee password caused the attack.	City + county offline Government Technology
Oct 2026	NEW **Maryland**	**Anne Arundel County confirms breach as Rhysida demands $2 million** The county confirmed an unauthorized actor accessed a small number of systems in August and copied some files. The Rhysida ransomware gang claimed the attack, demanded $2 million and threatened to leak 2.6 TB of documents.	2.6 TB claimed The Record
Oct 2026	NEW **Florida** 1M+ PEOPLE	**Florida student aid website breach may affect 4.9 million people** FLDOE announced unauthorized criminal access to the Florida Student Financial Aid website. Exposed data may include Social Security numbers, names, birth dates and addresses.	~4.9 million people WWSB ABC7
Oct 2026	NEW **Vermont**	**Slate Valley school district refuses ransom after data breach** Hackers accessed business documents and employee personal information in a September breach and demanded a ransom. On Oct. 2 the district said its board declined to pay on legal advice.	Employee data WCAX
Sep 2026	NEW **Phoenix, AZ** 1M+ PEOPLE	**Arizona court system hack copies data on 1.3 million people** Attackers who got in through a phishing email copied court records on 1.3 million people, including unpaid fines and restitution going back 30 years. The records also include nearly 30,000 protection orders and about 150,000 foster care board reports.	1.3M people KOLD News 13
Sep 2026	NEW **Wyoming** PRIORITY	**Court vendor breach exposes Wyoming court users' personal data** The Wyoming Judicial Branch said on Sept. 2, 2026, that court user data was obtained in a breach at its vendor, West Publishing Corporation, which also hit other court systems around the country. Names, addresses and dates of birth of people who dealt with district courts or the Supreme Court from 2015 to 2025 were compromised, and courts kept operating normally.	Court users, 2015-2025 Wyoming Public Media
Jun 2026	**District of Columbia**	**Cyberattack compromises D.C. Housing Authority systems, website down** On June 29, 2026, the D.C. Housing Authority was hit by a cyberattack that left its systems compromised, took its website offline and cut staff off from their files. It was not clear whether any personal information was exposed.	Agency website, files offline WJLA 7News
Mar 2026	**Idaho**	**Ransomware attack on Kootenai County exposes resident data** A ransomware attack detected March 30 hit Kootenai County's network, and the county found criminals took data that may include Social Security, ITIN and driver's license numbers. The county has not said how many residents were affected.	Resident data stolen Coeur d'Alene Press

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Jan 2026	**Connecticut**	**Cyberattack disrupts New Britain municipal systems** A cyberattack detected January 28, 2026, disrupted several New Britain municipal systems and may have exposed names, birth dates, ID numbers, financial and health-related information. The city offered credit monitoring; the number affected was unclear.	**Several city systems disrupted** Connecticut Public
2025			
Nov 2025	**Massachusetts**	**Attleboro intrusion may have exposed SSNs and medical data** Suspicious activity on Attleboro's network ran from October 22 to November 20, 2025, disrupting city systems. In October 2026 the city said exposed data may include Social Security, financial account, driver's license and medical information, and began mailing notices.	**Month-long intrusion** WJAR (NBC 10)
Sep 2025	**Augusta, GA** 1M+ PEOPLE	**Breach at Augusta medical billing vendor exposes 1.2 million+ patients** The PEAR extortion group was inside billing vendor MCBS's systems Sept. 22-26, 2025. It took names, Social Security numbers, insurance details and clinical records on more than 1.2 million people and published the data online.	**1.2M+ people** HotHardware
Sep 2025	**Illinois**	**IDHS maps exposed data on ~700,000 residents for years** Internal IDHS resource-planning maps were publicly viewable on a mapping website because of incorrect privacy settings, exposing addresses, case numbers and other details of Medicaid, Medicare Savings Program and rehabilitation services customers. IDHS found the problem on Sept. 22, 2025, restricted access by Sept. 26, and said it knew of no misuse.	**About 700,000 residents** BleepingComputer
Aug 2025	**Hawaii** 1M+ PEOPLE	**Ransomware hits UH Cancer Center, research data of 1.2M exposed** Attackers encrypted and stole Epidemiology Division research files, including Social Security numbers, driver's license data and 1998 Honolulu voter registration information. UHCC paid a ransom for a decryptor and data deletion; patient care was not affected.	**About 1.24M people** HIPAA Journal
Aug 2025	**Utah**	**Interlock ransomware steals Box Elder County data, 81,664 notified** Box Elder County found ransomware on Aug. 3, 2025, after unauthorized access that began in May. Interlock claimed 4.5 TB of data, and the county refused to pay and notified 81,664 people about exposed data, including Social Security numbers.	**81,664 people notified** Comparitech
Jul 2025	**Iowa City, IA** PRIORITY	**UI Health Care home care affiliate breach hits 211,000** Attackers got into UI Community HomeCare's network on July 3, 2025 and took files. Patient names, birth dates, medical record numbers, insurance details and, for some, Social Security numbers of about 211,000 people were exposed.	**~211,000 people** teiss
Jul 2025	**Maine**	**Cyberattack forces Bar Harbor offline, water plant controls cut** After detecting a cyberattack, Bar Harbor physically disconnected municipal systems, including controls that monitor its water and wastewater plants, and closed the town office. The town froze its bank accounts as a precaution and told employees personal data may have been accessed.	**Town services offline** Bangor Daily News
Jun 2025	**Lewiston, ME**	**Central Maine Healthcare breach exposes 145,381 patients** Attackers were in Central Maine Healthcare's systems from March to June 2025. Names, birth dates, Social Security numbers, treatment details and insurance information of 145,381 people were exposed.	**145,381 people** SecurityWeek

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Jun 2025	**Arizona**	**Attackers breach Arizona election candidate portal, post Khomeini image** An attacker uploaded code through the Secretary of State's candidate portal and replaced candidate photos on 2016-2024 election results pages with an image of Ayatollah Khomeini. Officials said with moderate confidence that Iran or its affiliates were responsible and that no voter data was accessed; the portal is separate from voter registration and results systems.	**Candidate portal shut down** Votebeat
May 2025	**Austin, TX**	**Compromised TxDOT account used to download 300,000 crash reports** Attackers used a compromised account in TxDOT's Crash Records Information System to download nearly 300,000 crash reports. The reports include names, addresses, driver's license and plate numbers, and car insurance policy numbers.	**~300,000 crash reports** Texas Department of Transportation
May 2025	**Alabama**	**State IT office investigates breach affecting state systems** Alabama's Office of Information Technology reported a significant security breach affecting certain state systems, detected on a Friday evening and disclosed May 12, 2025. Some state employee usernames and passwords were compromised; OIT said it believed no residents' personal information was retrieved.	**Employee credentials compromised** Government Technology
Mar 2025	**New Haven, CT** 1M+ PEOPLE	**Yale New Haven Health breach hits more than 5.5 million patients** Attackers copied patient data on March 8, 2025, including names, birth dates, addresses, Social Security numbers and medical record numbers. The HHS breach tracker lists more than 5.5 million people affected.	**5.5M+ patients** SecurityWeek
Feb 2025	**Aiken County, SC**	**Rural Health Services breach exposes 36,500 patients' SSNs and records** Attackers had network access from Jan. 15 to Feb. 13, 2025, exposing names with Social Security, driver's license, passport, and financial account numbers plus medical and insurance details. Up to 36,542 patients were affected.	**36,542 patients** The HIPAA Journal
Jan 2025	**Terre Haute, IN**	**Oracle Health hack exposes 262,831 Union Health patients** Attackers got into Oracle Health's data migration environment after Jan. 22, 2025 and took Union Health patient records. Social Security and driver's license numbers, insurance information, medications and diagnoses of 262,831 people may have been exposed.	**262,831 people** Becker's Hospital Review
Jan 2025	**Frederick, MD**	**Ransomware at Frederick Health exposes 934,326 patients** A ransomware attack detected on Jan. 27, 2025 stole names, addresses, Social Security and driver's license numbers, and for some, insurance and clinical information. Frederick Health reported 934,326 patients affected to HHS.	**934,326 patients** BleepingComputer
2024			
Dec 2024	**Rhode Island**	**Brain Cipher breach of RIBridges benefits system exposes 644,000 people** Brain Cipher used a stolen Deloitte credential to get into the state's RIBridges benefits system in July 2024 and stayed about five months before the state was notified in December 2024. Personal data of an estimated 644,401 applicants and recipients was compromised, and Deloitte has paid the state $12 million in total.	**644,401 people** Rhode Island Current
Nov 2024	**Concord, NH**	**Vendor hack exposes SSNs of nearly 68,000 Concord Orthopaedics patients** A breach at the practice's patient check-in software vendor exposed names, birth dates, Social Security numbers, insurance details, and some ID images. The Everest group listed the practice on its leak site; 67,835 New Hampshire residents were notified in March 2025.	**67,835 N.H. residents** DataBreaches.net

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Nov 2024	**Michigan**	**Ransomware gang hits Michigan county on Election Day** Wexford County's website was compromised on Election Day 2024, and the Embargo ransomware group claimed it stole 1 TB of data. County officials said election security and integrity were not affected and that staff stopped the encryption of county systems.	Claimed 1 TB stolen Comparitech
Oct 2024	**Charleston, WV**	**Phishing breach at CAMC exposes 67,000 patients' SSNs** A phishing attack let attackers into an employee mailbox Oct. 2-3, 2024, exposing names, birth dates, Social Security and driver's license numbers, and health and insurance details. At least 67,413 people were affected.	67,413 people TEISS
Oct 2024	**Colorado**	**Voting equipment BIOS passwords left exposed on state website** BIOS passwords for ballot tabulation equipment sat in a hidden spreadsheet tab on the Secretary of State's website from June until October 24, 2024. Officials called it accidental and said it posed no security threat given physical access controls; staff reset passwords in affected counties.	32 of 64 counties Colorado Public Radio
Oct 2024	**Wisconsin**	**Chort ransomware steals data on 67,000 Sheboygan residents** Hackers breached Sheboygan's systems on Oct. 31, 2024, and the Chort gang claimed the attack. About 67,000 people were affected, with exposed Social Security numbers, state IDs and license plate numbers.	~67,000 people The Record
Sep 2024	**Delaware**	**Ransomware disrupts Delaware public libraries statewide** A ransomware attack on a Delaware Libraries server knocked out internet, computer and some phone services at libraries across the state's 35-site system. A RansomHub affiliate claimed stolen data; officials rebuilt systems rather than pay, and said the patron catalog was not affected.	35-site system disrupted The Register
Aug 2024	**Anaconda, MT**	**Anaconda hospital breach exposes SSNs and medical data of 21,000** Attackers accessed the hospital's network Aug. 10-12, 2024, exposing names, Social Security numbers, financial account and Medicare/Medicaid numbers, and treatment and insurance details. The Meow ransomware gang claimed the attack; 21,243 people were affected.	21,243 people Comparitech
Aug 2024	**Washington**	**Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people** The Port of Seattle blamed Rhysida for an Aug. 24, 2024 attack that disrupted systems at Seattle-Tacoma International Airport. The Port refused a $6 million ransom and notified about 90,000 people.	90,000 people SecurityWeek
Jul 2024	**Dover, DE**	**Rhysida hack of Delaware's Bayhealth exposes 497,047 people** The Rhysida ransomware gang got into Bayhealth's network July 27-31, 2024 and copied files that may include Social Security numbers and medical and insurance information. Bayhealth reported 497,047 people affected to HHS.	497,047 people GovInfoSecurity
Jul 2024	**Woonsocket, RI**	**Human services agency breach exposes 115,000 Rhode Islanders' records** Attackers were inside the agency's network July 1-5, 2024, exposing names, Social Security and driver's license numbers, diagnoses, lab results, and insurance details. 114,975 people were affected; the Rhysida ransomware group listed the agency on its leak site.	114,975 people The HIPAA Journal
Jul 2024	**Florida**	**RansomHub leaks data stolen from Florida health department** A cyberattack on the Florida Department of Health disrupted its vital statistics system for birth and death certificates. RansomHub claimed 100 GB of stolen data and began leaking it after the state refused to pay.	100 GB claimed stolen GovInfoSecurity

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Jul 2024	**Kentucky**	**Ransomware shuts Jefferson County Clerk's offices for a week** A ransomware attack shut down the Louisville-area clerk's office from July 22 to July 29, closing motor vehicle branches. RansomHub later claimed the attack and said it stole election, motor vehicle and property data; the office had said no data was compromised and did not confirm the group.	**Offices closed ~1 week** Comparitech
Jul 2024	**Ohio**	**Rhysida ransomware exposes data of 500,000 Columbus residents** A July 2024 ransomware attack led Columbus to take critical systems offline, and the Rhysida group claimed it stole 6.5TB of data and posted 3.1TB. The city notified about 500,000 people whose data, including SSNs and bank details, may have been exposed.	**~500K people notified** Infosecurity Magazine
Jun 2024	**Montgomery, AL**	**Attack on Alabama education department exposes student, teacher data** Attackers got into Alabama State Department of Education systems on June 17, 2024. Data that may include names, addresses and Social Security numbers of students and educators was taken; the department has not given a count.	**Count not disclosed** Alabama Political Reporter
Jun 2024	**Madison, WI**	**Partner email hack exposes data of 19,000 Wisconsin Medicaid recipients** Attackers got into an employee email account at Disability Rights Wisconsin, a state health department partner, exposing protected health information. Up to 19,150 Medicaid recipients were notified in June 2024.	**19,150 people** The HIPAA Journal
May 2024	**Wichita, KS** PRIORITY	**LockBit ransomware steals data on 47,784 from City of Wichita** LockBit hit Wichita city systems in May 2024 and copied police incident and traffic records. Names, Social Security numbers and driver's license numbers of at least 47,784 people were taken.	**47,784 people** teiss
May 2024	**St. Louis, MO** 1M+ PEOPLE	**Ascension ransomware attack exposes data of 5.6 million people** Attackers copied files from St. Louis-based Ascension on May 7-8, 2024. Bank account and Social Security numbers, birth dates and some lab and billing details of 5.6 million patients, residents and employees were exposed.	**5.6M people** Fierce Healthcare
May 2024	**Albuquerque, NM**	**Law firm breach exposes 300,000 Presbyterian Healthcare patients** Attackers breached the network of Thompson Coburn, a law firm serving Presbyterian Healthcare, exposing patient names, Social Security numbers, birth dates, and treatment and insurance details. The firm reported 305,088 people affected to HHS.	**305,088 people** SecurityWeek
May 2024	**Kansas** PRIORITY	**Ransomware attackers steal personal, medical data from Franklin County** Franklin County said a ransomware attack on its network led cybercriminals to take data on May 19, 2024, including names, Social Security numbers, driver's license and financial account numbers, and medical and vaccination information. The county brought in a forensics team and federal law enforcement.	**Personal, medical data stolen** Insurance Journal
Apr 2024	**Oakland, CA** 1M+ PEOPLE	**Kaiser tracking code sent data on 13.4M members to advertisers** Tracking code on Kaiser Permanente's websites and apps sent member names, IP addresses, sign-in status and health encyclopedia searches to advertisers such as Google, Microsoft and X. The exposure affected 13.4 million current and former members and patients.	**13.4M members** TechCrunch
Apr 2024	**Charlotte, NC**	**Phishing attack on Atrium Health exposes 586,000 people** A phishing attack gave attackers access to employee email accounts on April 29-30, 2024, exposing Social Security numbers, birth dates, bank details, and treatment and insurance records. Atrium reported 585,959 people affected to HHS.	**585,959 people** TEISS

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Apr 2024	**Richmond, VA** 1M+ PEOPLE	**Radiology Associates of Richmond hack affects 1.4 million patients** Attackers accessed the practice's files in April 2024; notices went out starting July 2025, with credit monitoring offered to people whose Social Security numbers were included. More than 1.4 million patients were affected.	1.4M+ patients AuntMinnie
Mar 2024	**Springdale, AR**	**Hack of Arkansas mental health provider exposes 375,000 patients** Attackers got into Arisa Health's network March 1-18, 2024. Names, Social Security numbers, medical histories, diagnoses and substance abuse program records of 375,436 people may have been exposed.	375,436 people GovInfoSecurity
Feb 2024	**Newark, NJ** 1M+ PEOPLE	**Prudential breach exposes data of 2.5 million people** Attackers broke into Prudential's systems on Feb. 4, 2024, taking names, addresses, and driver's license or ID numbers. The company told the Maine Attorney General that 2,556,210 people were affected; the Alphv/BlackCat gang claimed the attack.	2.56M people SecurityWeek
Feb 2024	**Nebraska** PRIORITY	**Change Healthcare ransomware reaches 575,000+ Nebraskans** The attack on the national claims processor exposed data on about 190 million people. Nebraska's attorney general sued after finding at least 575,000 Nebraskans affected.	575,000+ Nebraskans Nebraska Examiner
Jan 2024	**Chicago, IL**	**Ransomware at Lurie Children's exposes 791,000 patients' data** Attackers were in Lurie Children's systems Jan. 26-31, 2024, and the Rhysida gang claimed the attack. Social Security numbers, driver's license numbers, diagnoses and treatment details of more than 791,000 people were exposed.	791,000+ people SecurityWeek
2023			
Dec 2023	**Cleveland, OH**	**Ohio Lottery ransomware attack exposes SSNs of 539,000** Attackers broke into the Ohio Lottery's internal network on Christmas Eve 2023, taking names and Social Security numbers. The DragonForce ransomware gang claimed the attack; 538,959 people were affected.	538,959 people Security Affairs
Nov 2023	**Idaho Falls, ID**	**Hacktivists steal HR data on 45,047 at Idaho nuclear lab** The SiegedSec hacktivist group claimed a Nov. 19, 2023 breach of INL's cloud HR system and leaked the data. Names, Social Security numbers, salaries and bank details of 45,047 current and former workers and family members were exposed.	45,047 people Security Affairs
Nov 2023	**Oklahoma City, OK** 1M+ PEOPLE	**Integris Health breach hits 2.4 million; patients get extortion emails** Attackers stole patient data from Oklahoma's Integris Health in a Nov. 28, 2023 attack and then emailed patients directly demanding $50 each. Integris reported about 2.39 million people affected to HHS.	~2.39M people Becker's Hospital Review
Oct 2023	**Bismarck, ND**	**Network intrusion at Dakota Eye Institute exposes 107,000 patients** Attackers broke into the eye clinic's network in October 2023, exposing names, birth dates, Social Security numbers, and medical and insurance information. 107,143 patients were affected.	107,143 patients The HIPAA Journal
Oct 2023	**District of Columbia**	**D.C. voter data stolen through a vendor server** Hackers took D.C. Board of Elections voter data from a server run by its website vendor. Officials said the attackers may have had access to the full voter roll.	Full voter roll at risk The Record
Oct 2023	**Kansas** PRIORITY	**Kansas court system hit by foreign cyberattack** Officials called it a sophisticated foreign cyberattack. Courts in 104 counties were disrupted for weeks, electronic filing went down, and files and case records were stolen.	104 counties disrupted WIBW

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Oct 2023	**Nevada**	**Unauthorized party breaches Clark County schools email system** Around Oct. 5, 2023, an unauthorized party got into the district's email environment and accessed limited personal information on a subset of students, parents and employees. The district brought in forensic experts, worked with law enforcement and required students to change their passwords.	**Subset of students, staff** News 3 Las Vegas (KSNV)
Sep 2023	**Reno, NV**	**Caesars hack exposes loyalty members' driver's license data** Attackers had network access starting Aug. 18, 2023, and took data including names with driver's license or ID numbers. The Maine filing lists 41,397 Maine residents alone; the total was listed as still to be determined.	**41,397 Maine residents; total TBD** Maine Attorney General
Aug 2023	**Grand Blanc, MI** 1M+ PEOPLE	**McLaren Health Care breach exposes 2.2 million people** Attackers were in McLaren's network July 28-Aug. 23, 2023, and the ALPHV/BlackCat gang listed it on its leak site. Names, Social Security numbers, insurance details, diagnoses and prescription records of about 2.2 million people were exposed.	**~2.2M people** SecurityWeek
Aug 2023	**Pascagoula, MS**	**Rhysida attack on Singing River Health System hits 895,204** The Rhysida ransomware group hit Singing River's three Gulf Coast hospitals in August 2023. Names, birth dates, addresses, Social Security numbers, and medical and insurance information of 895,204 people were exposed.	**895,204 people** Security Affairs
Jul 2023	**St. Landry Parish, LA**	**Medusa leaks St. Landry Parish schools data; families never notified** The Medusa ransomware group leaked about 211,000 St. Landry Parish school files in August 2023 after the district refused to pay. The files held Social Security numbers of at least 13,500 people, records on 2,700+ students and scanned birth and death certificates.	**13,500+ SSNs; 211,000 files** The 74
Jul 2023	**Nashville, TN** 1M+ PEOPLE	**HCA Healthcare breach exposes data of 11 million patients** Attackers took patient names, addresses, birth dates, contact details, and appointment information from an external storage location used for email formatting, and offered it for sale online. About 11 million patients were affected.	**~11M patients** SiliconANGLE
Jun 2023	**Anchorage, AK**	**Cyberattack on Alaska behavioral health provider hits 284,000** Attackers took administrative files from Akeela, an Alaska behavioral health nonprofit, around June 22, 2023. Names, birth dates, diagnosis and treatment details and Social Security numbers of more than 284,000 people were exposed.	**284,000+ people** HIPAA Journal
Jun 2023	**Denver, CO**	**Ransomware exposes 16 years of Colorado student and teacher records** Ransomware attackers were inside Colorado Department of Higher Education systems from June 11-19, 2023. They stole names, Social Security numbers, birth dates and ID copies for public college and high school students from 2004-2020 and for some educators; no total count was given.	**Count not disclosed** BleepingComputer
Jun 2023	**Hawaii County, HI**	**Hawaii Community College pays ransom after data on 28,000 stolen** The NoEscape ransomware group hit Hawaii Community College in June 2023, compromising personal information of more than 28,000 people. The college paid the attackers to keep the data from being leaked.	**28,000+ people** The Record
Jun 2023	**New York, NY**	**MOVEit hack exposes data of 45,000 NYC students** Attackers exploiting the MOVEit file-transfer flaw accessed about 19,000 documents, possibly including Social Security numbers, student ID numbers, birth dates, and Medicaid reports. About 45,000 students plus staff were affected.	**~45,000 students** Chalkbeat

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Jun 2023	**California**	**MOVEit breach exposes data of 769,000 CalPERS retirees** A CalPERS vendor was breached through the MOVEit file-transfer flaw, exposing retirees' and beneficiaries' names, birth dates and Social Security numbers. Officials attributed the theft to Russian cybercriminals; the report names the Cl0p group as behind the MOVEit campaign.	**About 769,000 people** KPBS (AP)
Jun 2023	**Louisiana** 1M+ PEOPLE	**MOVEit breach exposes records of nearly every Louisiana driver** Hackers breached the OMV's MOVEit file transfer system, exposing names, addresses, license photos, height and weight. The OMV believes everyone with a state license, ID or vehicle registration likely had data exposed.	**6M+ records** WAFB
Jun 2023	**Missouri**	**MOVEit breach via IBM exposes Missouri Medicaid data** Data was stolen through a MOVEit vulnerability in a tool IBM used for DSS, exposing Medicaid participants' names, client numbers, birth dates and claims data. DSS planned to notify all Medicaid participants and providers enrolled in May 2023.	**All Medicaid enrollees** The Record
Jun 2023	**Oregon** 1M+ PEOPLE	**MOVEit hack exposes 3.5M Oregon driver's license records** Attackers exploited the MOVEit file transfer tool used by ODOT and accessed files with names, license or ID numbers, birth dates, addresses and partial SSNs. The data covers about 3.5 million current Oregon license and ID holders; Cl0p claimed the MOVEit attack.	**3.5M records** Oregon DOT (official notice)
May 2023	**Tampa, FL** 1M+ PEOPLE	**Tampa General Hospital hack exposes data of 1.2 million patients** Attackers got into Tampa General's network May 12-30, 2023 and took files on about 1.2 million patients. The files included names, Social Security numbers, insurance details, medical record numbers and limited treatment information.	**1.2M patients** Infosecurity Magazine
May 2023	**Louisville, KY** 1M+ PEOPLE	**Norton Healthcare attack exposes data on 2.5 million people** Attackers got into Norton Healthcare's network storage in May 2023. They took Social Security numbers, health and insurance information and some financial account numbers of about 2.5 million patients, employees and dependents.	**~2.5M people** Malwarebytes
May 2023	**Roseville, MN**	**MOVEit hack exposes data on 95,000 Minnesota foster care students** Attackers used a MOVEit flaw on May 31, 2023 to get 24 education department files, and the CL0P group was behind the wider MOVEit campaign. Names, birth dates and placement counties of about 95,000 students in foster care were exposed.	**~95,000 students** FOX 9
May 2023	**Portland, OR** 1M+ PEOPLE	**MOVEit hack at Medicaid contractor exposes 1.7M Oregon Health Plan members** Attackers exploited the MOVEit flaw at PH Tech, a contractor for Oregon's Medicaid insurers, on May 30, 2023. Names, birth dates, Social Security numbers, and diagnosis and claims data of about 1.7 million current and former members were exposed.	**~1.7M members** Ashland.news
May 2023	**Colorado** 1M+ PEOPLE	**MOVEit breach exposes data of 4 million Colorado Medicaid members** An unauthorized party accessed HCPF files that service provider IBM was transferring with MOVEit, exposing names, Social Security numbers, medical and insurance information of Health First Colorado and CHP+ members. HCPF said its own systems were not impacted.	**About 4.1M people** SecurityWeek
May 2023	**Maine** 1M+ PEOPLE	**MOVEit breach hits roughly the entire population of Maine** Attackers exploited a zero-day in the state's MOVEit server on May 28-29, stealing files tied to health and human services, education, motor vehicles, corrections, unemployment and other agencies. Maine disclosed in November that about 1.3 million people were affected.	**1.3M people** Cybersecurity Dive

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Apr 2023	**Canton, MA** 1M+ PEOPLE	**Harvard Pilgrim ransomware attack exposes 2.86 million people** Ransomware attackers copied data from Harvard Pilgrim systems March 28-April 17, 2023. Social Security numbers, financial account and insurance information, and medical histories of more than 2.86 million people were exposed.	2.86M+ people SecurityWeek
Apr 2023	**Sioux Falls, SD** PRIORITY	**Imaging vendor breach exposes 21,000 Sanford Health patients** A breach at DMS Health Technologies, Sanford's mobile heart-screening imaging vendor, between March 27 and April 24, 2023, exposed patient names, birth dates, service dates, and exam types. More than 21,000 Sanford patients were notified.	21,000+ patients Becker's Hospital Review
Mar 2023	**Washington, DC**	**DC Health Link data on 56,415 people, including lawmakers, leaked** Data on 56,415 DC Health Link customers, including members of Congress and their staff, was posted and offered for sale on a crime forum. It included Social Security numbers, birth dates, addresses, employers and health plan details.	56,415 people FOX 5 DC
Feb 2023	**Allentown, PA**	**BlackCat ransomware steals patient records and photos from LVHN** The Alphv/BlackCat gang was inside the network from early January 2023 and deployed ransomware in February, stealing medical, insurance, and some Social Security and bank data plus clinical patient photos. Over 130,000 patients and employees were affected.	130,000+ people SecurityWeek
Feb 2023	**Minnesota**	**Medusa leaks Minneapolis schools data after $1M demand** The Medusa ransomware group attacked the district, demanded $1 million, and posted stolen data when it refused to pay. The leak reportedly included student records, health and disciplinary files, addresses, and payroll data.	34,500-student district The Record
Feb 2023	**West Virginia**	**Cyberattack cancels classes for 20,000 Berkeley County students** A cyberattack caused internet and phone outages at West Virginia's second-largest school district, and classes were canceled for nearly 20,000 students. The district said it did not know at the time whether personal data was breached.	~20,000 students out The Record
Jan 2023	**Bellevue, WA** 1M+ PEOPLE	**T-Mobile API abuse exposes 37 million customer accounts** Attackers pulled customer data through a single T-Mobile API, exposing names, billing addresses, emails, phone numbers, birth dates, and account numbers. About 37 million accounts were affected; T-Mobile said SSNs and payment data were not.	~37M accounts Security Affairs
Jan 2023	**Iowa** PRIORITY	**Des Moines Public Schools hit by ransomware** Iowa's largest school district took its network offline after a ransomware attack. Personal data of nearly 6,700 people was taken.	~6,700 people District Administration
Jan 2023	**Hawaii**	**Stolen login used to access Hawaii death registry records** Credentials for an unused external death certifier account were sold on the dark web and used to access the state's Electronic Death Registry System. Records exposed names, Social Security numbers, addresses and causes of death; the attacker has not been identified.	About 3,400 records The Record
2022			
Sep 2022	**New York**	**BlackCat ransomware cripples Suffolk County government** Attackers entered through the county clerk's office via Log4j in December 2021 and deployed ransomware in September 2022, disabling email for over 10,000 workers and forcing dispatchers to take calls by hand for weeks. About 400GB of stolen data was leaked; the BlackCat/AlphV group claimed the attack and the county did not pay.	~$5.5M cost; 400GB leaked The Record
2021			

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
May 2021	**Alaska**	**Nation-state attackers breach Alaska health department network** Attackers the department described as a nation-state sponsored group entered DHSS's internal network through a website vulnerability. Breached systems stayed offline for months, forcing manual processing of background checks and vital records, and any data on the agency's systems may have been exposed.	**Systems offline for months** The Record
May 2021	**Oklahoma**	**Tulsa ransomware shuts city services, leaks 18,000 files** Ransomware hit Tulsa's online bill payment, utility billing, email, websites, police and 311 systems, and the city shut down all services to stop the spread. After the city refused to pay, attackers leaked more than 18,000 files, mostly police citations and employee files.	**18,000+ files leaked** Route Fifty
Apr 2021	**Wyoming** PRIORITY	**Wyoming health test data posted to public GitHub** A Wyoming Department of Health employee uploaded files to GitHub that held lab test results for 164,021 people, about one in four state residents.	**164,021 people** Wyoming Department of Health
Feb 2021	**Washington** 1M+ PEOPLE	**Accellion breach may expose 1.6M Washington jobless claims** Attackers compromised Accellion file-transfer software used by the State Auditor. Names, Social Security numbers and bank information of about 1.6 million people who filed for unemployment in 2020 may have been exposed.	**1.6M claimants** Northwest Public Broadcasting
2020			
Oct 2020	**Alaska**	**Hackers steal Alaska voter data from online registration system** Outside actors gained unauthorized access to data in Alaska's online voter registration system, exposing names, birth dates, driver's license numbers, addresses, party affiliations and partial Social Security numbers. Officials said the breach did not affect election results and that no other election systems were affected.	**100,000+ voters** Alaska Public Media
Jul 2020	**Utah**	**University of Utah pays $457,000 after ransomware attack** Attackers encrypted servers in the university's College of Social and Behavioral Science and stole student and employee data first. The university's cyber insurer paid $457,059 to stop the data from being released.	**$457K ransom paid** BleepingComputer
2019			
Jan 2019	**Oregon**	**Phishing exposes data of 645,000 Oregon DHS clients** Nine DHS employees fell for a phishing email, giving an attacker access to mailboxes holding up to two million emails for about 20 days. Exposed data included names, SSNs, birth dates and protected health information.	**645,000 people** BleepingComputer
2017			
Mar 2017	**Vermont**	**Joblink breach puts unemployment filers' SSNs at risk** A breach of Joblink, the job-search database Vermont unemployment filers must use, may have exposed Social Security numbers. The vendor, America's Job Link Alliance, said more than 180,000 accounts were compromised, including tens of thousands of Vermonters.	**180,000+ accounts** Vermont Public
2016			
Jun 2016	**Illinois**	**Illinois voter registration database breached** Russian military intelligence officers accessed the Illinois State Board of Elections voter registration database, according to the Senate Intelligence Committee. State officials notified affected voters.	**Statewide voter rolls** CBS Chicago

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
2016	**Florida**	**Russian-linked hackers accessed voter data in two Florida counties** Gov. Ron DeSantis said in 2019 that Russia-affiliated actors accessed voter databases in two counties in 2016 via phishing emails posing as vendor VR Systems. He said the data was publicly available and the breach did not affect votes or results; the counties were not named.	**2 county voter databases** WFSU

JURISDICTION PROFILES · 50 STATES + D.C.

Every state, on one page

2024 FTC identity theft and fraud figures, and every documented breach of sensitive records in each jurisdiction.

Alabama AL · South

#17 of 51

13,596	269	$104.2M
ID THEFT	PER 100K	FRAUD LOSSES

May 2025 State IT office investigates breach affecting state systems. Government Technology

Jun 2024 Attack on Alabama education department exposes student, teacher data. Alabama Political Reporter

Alaska AK · West

#49 of 51

780	106	$26.9M
ID THEFT	PER 100K	FRAUD LOSSES

Jun 2023 Cyberattack on Alaska behavioral health provider hits 284,000. HIPAA Journal

May 2021 Nation-state attackers breach Alaska health department network. The Record

Oct 2020 Hackers steal Alaska voter data from online registration system. Alaska Public Media

Arizona AZ · West

#16 of 51

20,863	287	$336.7M
ID THEFT	PER 100K	FRAUD LOSSES

Sep 2026 NEW Arizona court system hack copies data on 1.3 million people. KOLD News 13

Jun 2025 Attackers breach Arizona election candidate portal, post Khomeini image. Votebeat

Arkansas AR · South

#26 of 51

6,340	209	$52.1M
ID THEFT	PER 100K	FRAUD LOSSES

Mar 2024 Hack of Arkansas mental health provider exposes 375,000 patients. GovInfoSecurity

California CA · West

#8 of 51

139,665	356	$1.68B
ID THEFT	PER 100K	FRAUD LOSSES

Apr 2024 Kaiser tracking code sent data on 13.4M members to advertisers. TechCrunch

Jun 2023 MOVEit breach exposes data of 769,000 CalPERS retirees. KPBS (AP)

Colorado CO · West

#27 of 51

12,087	208	$210.7M
ID THEFT	PER 100K	FRAUD LOSSES

Oct 2024 Voting equipment BIOS passwords left exposed on state website. Colorado Public Radio

Jun 2023 Ransomware exposes 16 years of Colorado student and teacher records. BleepingComputer

May 2023 MOVEit breach exposes data of 4 million Colorado Medicaid members. SecurityWeek

Connecticut CT · Northeast

#22 of 51

8,502	236	$90.3M
ID THEFT	PER 100K	FRAUD LOSSES

Jan 2026 Cyberattack disrupts New Britain municipal systems. Connecticut Public

Mar 2025 Yale New Haven Health breach hits more than 5.5 million patients. SecurityWeek

Delaware DE · South

#6 of 51

3,942	392	$34.3M
ID THEFT	PER 100K	FRAUD LOSSES

Sep 2024 Ransomware disrupts Delaware public libraries statewide. The Register

Jul 2024 Rhysida hack of Delaware's Bayhealth exposes 497,047 people. GovInfoSecurity

District of Columbia DC · South #3 of 51

3,225	480	$30.4M
ID THEFT	PER 100K	FRAUD LOSSES

- Jun 2026 Cyberattack compromises D.C. Housing Authority systems, website down. WJLA 7News
- Oct 2023 D.C. voter data stolen through a vendor server. The Record
- Mar 2023 DC Health Link data on 56,415 people, including lawmakers, leaked. FOX 5 DC

Florida FL · South #1 of 51

115,840	528	$866.1M
ID THEFT	PER 100K	FRAUD LOSSES

- Oct 2026 NEW Florida student aid website breach may affect 4.9 million people. WWSB ABC7
- Jul 2024 RansomHub leaks data stolen from Florida health department. GovInfoSecurity
- May 2023 Tampa General Hospital hack exposes data of 1.2 million patients. Infosecurity Magazine
- 2016 Russian-linked hackers accessed voter data in two Florida counties. WFSU

Georgia GA · South #2 of 51

55,955	517	$291.3M
ID THEFT	PER 100K	FRAUD LOSSES

- Sep 2025 Breach at Augusta medical billing vendor exposes 1.2 million+ patients. HotHardware

Hawaii HI · West #39 of 51

1,990	138	$61.6M
ID THEFT	PER 100K	FRAUD LOSSES

- Aug 2025 Ransomware hits UH Cancer Center, research data of 1.2M exposed. HIPAA Journal
- Jun 2023 Hawaii Community College pays ransom after data on 28,000 stolen. The Record
- Jan 2023 Stolen login used to access Hawaii death registry records. The Record

Idaho ID · West #44 of 51

2,367	125	$53.9M
ID THEFT	PER 100K	FRAUD LOSSES

- Mar 2026 Ransomware attack on Kootenai County exposes resident data. Coeur d'Alene Press
- Nov 2023 Hacktivists steal HR data on 45,047 at Idaho nuclear lab. Security Affairs

Illinois IL · Midwest #10 of 51

43,028	339	$318.1M
ID THEFT	PER 100K	FRAUD LOSSES

- Sep 2025 IDHS maps exposed data on ~700,000 residents for years. BleepingComputer
- Jan 2024 Ransomware at Lurie Children's exposes 791,000 patients' data. SecurityWeek
- Jun 2016 Illinois voter registration database breached. CBS Chicago

Indiana IN · Midwest #28 of 51

13,471	198	$112.3M
ID THEFT	PER 100K	FRAUD LOSSES

- Jan 2025 Oracle Health hack exposes 262,831 Union Health patients. Becker's Hospital Review

Iowa IA · Midwest · Priority #45 of 51

3,919	123	$52.0M
ID THEFT	PER 100K	FRAUD LOSSES

- Jul 2025 UI Health Care home care affiliate breach hits 211,000. teiss
- Jan 2023 Des Moines Public Schools hit by ransomware. District Administration

Kansas KS · Midwest · Priority #34 of 51

4,518	154	$57.6M
ID THEFT	PER 100K	FRAUD LOSSES

- May 2024 LockBit ransomware steals data on 47,784 from City of Wichita. teiss
- May 2024 Ransomware attackers steal personal, medical data from Franklin County. Insurance Journal
- Oct 2023 Kansas court system hit by foreign cyberattack. WIBW

Kentucky KY · South

#38 of 51

6,396	142	$70.8M
ID THEFT	PER 100K	FRAUD LOSSES

Jul 2024 Ransomware shuts Jefferson County Clerk's offices for a week. Comparitech

May 2023 Norton Healthcare attack exposes data on 2.5 million people. Malwarebytes

Louisiana LA · South

#9 of 51

15,991	346	$89.4M
ID THEFT	PER 100K	FRAUD LOSSES

Jul 2023 Medusa leaks St. Landry Parish schools data; families never notified. The 74

Jun 2023 MOVEit breach exposes records of nearly every Louisiana driver. WAFB

Maine ME · Northeast

#42 of 51

1,746	127	$29.3M
ID THEFT	PER 100K	FRAUD LOSSES

Jul 2025 Cyberattack forces Bar Harbor offline, water plant controls cut. Bangor Daily News

Jun 2025 Central Maine Healthcare breach exposes 145,381 patients. SecurityWeek

May 2023 MOVEit breach hits roughly the entire population of Maine. Cybersecurity Dive

Maryland MD · South

#11 of 51

19,990	324	$198.9M
ID THEFT	PER 100K	FRAUD LOSSES

Oct 2026 NEW Anne Arundel County confirms breach as Rhysida demands $2 million. The Record

Jan 2025 Ransomware at Frederick Health exposes 934,326 patients. BleepingComputer

Massachusetts MA · Northeast

#7 of 51

27,141	388	$210.3M
ID THEFT	PER 100K	FRAUD LOSSES

Nov 2025 Attleboro intrusion may have exposed SSNs and medical data. WJAR (NBC 10)

Apr 2023 Harvard Pilgrim ransomware attack exposes 2.86 million people. SecurityWeek

Michigan MI · Midwest

#21 of 51

23,783	237	$204.0M
ID THEFT	PER 100K	FRAUD LOSSES

Nov 2024 Ransomware gang hits Michigan county on Election Day. Comparitech

Aug 2023 McLaren Health Care breach exposes 2.2 million people. SecurityWeek

Minnesota MN · Midwest

#43 of 51

7,280	127	$144.6M
ID THEFT	PER 100K	FRAUD LOSSES

May 2023 MOVEit hack exposes data on 95,000 Minnesota foster care students. FOX 9

Feb 2023 Medusa leaks Minneapolis schools data after $1M demand. The Record

Mississippi MS · South

#18 of 51

7,903	268	$44.4M
ID THEFT	PER 100K	FRAUD LOSSES

Aug 2023 Rhysida attack on Singing River Health System hits 895,204. Security Affairs

Missouri MO · Midwest

#29 of 51

11,535	187	$139.3M
ID THEFT	PER 100K	FRAUD LOSSES

May 2024 Ascension ransomware attack exposes data of 5.6 million people. Fierce Healthcare

Jun 2023 MOVEit breach via IBM exposes Missouri Medicaid data. The Record

Montana MT · West

#40 of 51

1,447	131	$22.5M
ID THEFT	PER 100K	FRAUD LOSSES

Aug 2024 Anaconda hospital breach exposes SSNs and medical data of 21,000. Comparitech

Nebraska NE · Midwest · Priority

#41 of 51

2,554	130	$41.9M
ID THEFT	PER 100K	FRAUD LOSSES

Oct 2026 NEW North Platte and Lincoln County, Neb., knocked offline. Government Technology

Feb 2024 Change Healthcare ransomware reaches 575,000+ Nebraskans. Nebraska Examiner

Nevada NV · West

#4 of 51

14,631	466	$138.5M
ID THEFT	PER 100K	FRAUD LOSSES

Oct 2023 Unauthorized party breaches Clark County schools email system. News 3 Las Vegas (KSNV)

Sep 2023 Caesars hack exposes loyalty members' driver's license data. Maine Attorney General

New Hampshire NH · Northeast

#36 of 51

2,079	150	$34.6M
ID THEFT	PER 100K	FRAUD LOSSES

Nov 2024 Vendor hack exposes SSNs of nearly 68,000 Concord Orthopaedics patients. DataBreaches.net

New Jersey NJ · Northeast

#12 of 51

29,037	313	$314.4M
ID THEFT	PER 100K	FRAUD LOSSES

Feb 2024 Prudential breach exposes data of 2.5 million people. SecurityWeek

New Mexico NM · West

#35 of 51

3,171	150	$56.6M
ID THEFT	PER 100K	FRAUD LOSSES

May 2024 Law firm breach exposes 300,000 Presbyterian Healthcare patients. SecurityWeek

New York NY · Northeast

#13 of 51

58,692	295	$534.0M
ID THEFT	PER 100K	FRAUD LOSSES

Jun 2023 MOVEit hack exposes data of 45,000 NYC students. Chalkbeat

Sep 2022 BlackCat ransomware cripples Suffolk County government. The Record

North Carolina NC · South

#20 of 51

27,466	259	$276.8M
ID THEFT	PER 100K	FRAUD LOSSES

Apr 2024 Phishing attack on Atrium Health exposes 586,000 people. TEISS

North Dakota ND · Midwest

#47 of 51

924	119	$14.4M
ID THEFT	PER 100K	FRAUD LOSSES

Oct 2023 Network intrusion at Dakota Eye Institute exposes 107,000 patients. The HIPAA Journal

Ohio OH · Midwest

#23 of 51

27,766	236	$226.2M
ID THEFT	PER 100K	FRAUD LOSSES

Jul 2024 Rhysida ransomware exposes data of 500,000 Columbus residents. Infosecurity Magazine

Dec 2023 Ohio Lottery ransomware attack exposes SSNs of 539,000. Security Affairs

Oklahoma OK · South

#30 of 51

6,747	169	$72.7M
ID THEFT	PER 100K	FRAUD LOSSES

Nov 2023 Integris Health breach hits 2.4 million; patients get extortion emails. Becker's Hospital Review

May 2021 Tulsa ransomware shuts city services, leaks 18,000 files. Route Fifty

Oregon OR · West

#32 of 51

6,898	163	$123.7M
ID THEFT	PER 100K	FRAUD LOSSES

Jun 2023 MOVEit hack exposes 3.5M Oregon driver's license records. Oregon DOT (official notice)

May 2023 MOVEit hack at Medicaid contractor exposes 1.7M Oregon Health Plan members. Ashland.news

Jan 2019 Phishing exposes data of 645,000 Oregon DHS clients. BleepingComputer

Pennsylvania PA · Northeast

#15 of 51

ID THEFT	PER 100K	FRAUD LOSSES
37,717	290	$285.4M

Feb 2023 BlackCat ransomware steals patient records and photos from LVHN. SecurityWeek

Rhode Island RI · Northeast

#19 of 51

ID THEFT	PER 100K	FRAUD LOSSES
2,896	264	$20.7M

Dec 2024 Brain Cipher breach of RIBridges benefits system exposes 644,000 people. Rhode Island Current

Jul 2024 Human services agency breach exposes 115,000 Rhode Islanders' records. The HIPAA Journal

South Carolina SC · South

#14 of 51

ID THEFT	PER 100K	FRAUD LOSSES
15,146	291	$137.0M

Feb 2025 Rural Health Services breach exposes 36,500 patients' SSNs and records. The HIPAA Journal

South Dakota SD · Midwest ·

#51 of 51

Priority

ID THEFT	PER 100K	FRAUD LOSSES
845	94	$20.4M

Apr 2023 Imaging vendor breach exposes 21,000 Sanford Health patients. Becker's Hospital Review

Tennessee TN · South

#25 of 51

ID THEFT	PER 100K	FRAUD LOSSES
14,829	212	$157.2M

Jul 2023 HCA Healthcare breach exposes data of 11 million patients. SiliconANGLE

Texas TX · South

#5 of 51

ID THEFT	PER 100K	FRAUD LOSSES
116,484	393	$897.9M

May 2025 Compromised TxDOT account used to download 300,000 crash reports. Texas Department of Transportation

Utah UT · West

#33 of 51

ID THEFT	PER 100K	FRAUD LOSSES
5,224	157	$113.1M

Aug 2025 Interlock ransomware steals Box Elder County data, 81,664 notified. Comparitech

Jul 2020 University of Utah pays $457,000 after ransomware attack. BleepingComputer

Vermont VT · Northeast

#50 of 51

ID THEFT	PER 100K	FRAUD LOSSES
651	101	$10.6M

Oct 2026 NEW Slate Valley school district refuses ransom after data breach. WCAX

Mar 2017 Joblink breach puts unemployment filers' SSNs at risk. Vermont Public

Virginia VA · South

#24 of 51

ID THEFT	PER 100K	FRAUD LOSSES
18,460	213	$293.7M

Apr 2024 Radiology Associates of Richmond hack affects 1.4 million patients. AuntMinnie

Washington WA · West

#31 of 51

ID THEFT	PER 100K	FRAUD LOSSES
13,068	169	$297.2M

Aug 2024 Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people. SecurityWeek

Jan 2023 T-Mobile API abuse exposes 37 million customer accounts. Security Affairs

Feb 2021 Accellion breach may expose 1.6M Washington jobless claims. Northwest Public Broadcasting

West Virginia WV · South

#48 of 51

ID THEFT	PER 100K	FRAUD LOSSES
2,017	113	$27.0M

Oct 2024 Phishing breach at CAMC exposes 67,000 patients' SSNs. TEISS

Feb 2023 Cyberattack cancels classes for 20,000 Berkeley County students. The Record

WISCONSIN WI · Midwest #37 of 51

8,798	149	$106.0M
ID THEFT	PER 100K	FRAUD LOSSES

> **Oct 2024** Chort ransomware steals data on 67,000 Sheboygan residents. The Record

> **Jun 2024** Partner email hack exposes data of 19,000 Wisconsin Medicaid recipients. The HIPAA Journal

WYOMING WY · West · Priority #46 of 51

697	120	$20.1M
ID THEFT	PER 100K	FRAUD LOSSES

> **Sep 2026** NEW Court vendor breach exposes Wyoming court users' personal data. Wyoming Public Media

> **Apr 2021** Wyoming health test data posted to public GitHub. Wyoming Department of Health

ENGAGEMENT PLAN

From a data map to proven recovery

Read-only first. Nothing touches a live system until the state approves.

PHASE 1 · 90 DAYS

Map the data

- Inventory sensitive data sets, owners and legal bases.
- Vendor, subcontractor and broker map from contracts.
- Read-only review; no live systems touched.

PHASE 2 · 2027

Prove recovery

- Sovereign server plane stood up for one agency.
- First timed restore drill on synthetic data.
- WAYBILL logging on every outbound transfer.

PHASE 3 · 2027 – 2028

Scale

- Every agency on BACKSTOP 3-2-1 with quarterly drills.
- Retention clocks and verified destruction statewide.
- Same receipts and audit trail in every state.

BB2G
BORN BETWEEN 2 GENERALS

Decision requested

Authorize a read-only data inventory of one agency to set owners, legal bases, safeguards and a restore-time target.

SOURCES

Trace every figure

1. Federal Trade Commission, Consumer Sentinel Network Data Book 2024
2. Federal Trade Commission, testimony to the Joint Economic Committee, March 2026 (2025 fraud losses)
3. U.S. Census Bureau, Vintage 2025 state population estimates
4. HHS Office for Civil Rights, breach portal
5. NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
6. CISA #StopRansomware Guide (offline, encrypted backups)
7. **AL** Alabama Political Reporter, “Attack on Alabama education department exposes student, teacher data” (Jun 2024)
8. **AL** Government Technology, “State IT office investigates breach affecting state systems” (May 2025)
9. **AK** Alaska Public Media, “Hackers steal Alaska voter data from online registration system” (Oct 2020)
10. **AK** The Record, “Nation-state attackers breach Alaska health department network” (May 2021)
11. **AK** HIPAA Journal, “Cyberattack on Alaska behavioral health provider hits 284,000” (Jun 2023)
12. **AZ** Votebeat, “Attackers breach Arizona election candidate portal, post Khomeini image” (Jun 2025)
13. **AZ** KOLD News 13, “Arizona court system hack copies data on 1.3 million people” (Sep 2026)
14. **AR** GovInfoSecurity, “Hack of Arkansas mental health provider exposes 375,000 patients” (Mar 2024)
15. **CA** KPBS (AP), “MOVEit breach exposes data of 769,000 CalPERS retirees” (Jun 2023)
16. **CA** TechCrunch, “Kaiser tracking code sent data on 13.4M members to advertisers” (Apr 2024)
17. **CO** SecurityWeek, “MOVEit breach exposes data of 4 million Colorado Medicaid members” (May 2023)
18. **CO** BleepingComputer, “Ransomware exposes 16 years of Colorado student and teacher records” (Jun 2023)
19. **CO** Colorado Public Radio, “Voting equipment BIOS passwords left exposed on state website” (Oct 2024)
20. **CT** SecurityWeek, “Yale New Haven Health breach hits more than 5.5 million patients” (Mar 2025)
21. **CT** Connecticut Public, “Cyberattack disrupts New Britain municipal systems” (Jan 2026)
22. **DE** GovInfoSecurity, “Rhysida hack of Delaware's Bayhealth exposes 497,047 people” (Jul 2024)
23. **DE** The Register, “Ransomware disrupts Delaware public libraries statewide” (Sep 2024)
24. **DC** FOX 5 DC, “DC Health Link data on 56,415 people, including lawmakers, leaked” (Mar 2023)
25. **DC** The Record, “D.C. voter data stolen through a vendor server” (Oct 2023)
26. **DC** WJLA 7News, “Cyberattack compromises D.C. Housing Authority systems, website down” (Jun 2026)
27. **FL** WFSU, “Russian-linked hackers accessed voter data in two Florida counties” (2016)
28. **FL** Infosecurity Magazine, “Tampa General Hospital hack exposes data of 1.2 million patients” (May 2023)
29. **FL** GovInfoSecurity, “RansomHub leaks data stolen from Florida health department” (Jul 2024)
30. **FL** WWSB ABC7, “Florida student aid website breach may affect 4.9 million people” (Oct 2026)

31. **GA** HotHardware, “Breach at Augusta medical billing vendor exposes 1.2 million+ patients” (Sep 2025)
32. **HI** The Record, “Stolen login used to access Hawaii death registry records” (Jan 2023)
33. **HI** The Record, “Hawaii Community College pays ransom after data on 28,000 stolen” (Jun 2023)
34. **HI** HIPAA Journal, “Ransomware hits UH Cancer Center, research data of 1.2M exposed” (Aug 2025)
35. **ID** Security Affairs, “Hacktivists steal HR data on 45,047 at Idaho nuclear lab” (Nov 2023)
36. **ID** Coeur d'Alene Press, “Ransomware attack on Kootenai County exposes resident data” (Mar 2026)
37. **IL** CBS Chicago, “Illinois voter registration database breached” (Jun 2016)
38. **IL** SecurityWeek, “Ransomware at Lurie Children's exposes 791,000 patients' data” (Jan 2024)
39. **IL** BleepingComputer, “IDHS maps exposed data on ~700,000 residents for years” (Sep 2025)
40. **IN** Becker's Hospital Review, “Oracle Health hack exposes 262,831 Union Health patients” (Jan 2025)
41. **IA** District Administration, “Des Moines Public Schools hit by ransomware” (Jan 2023)
42. **IA** teiss, “UI Health Care home care affiliate breach hits 211,000” (Jul 2025)
43. **KS** WIBW, “Kansas court system hit by foreign cyberattack” (Oct 2023)
44. **KS** teiss, “LockBit ransomware steals data on 47,784 from City of Wichita” (May 2024)
45. **KS** Insurance Journal, “Ransomware attackers steal personal, medical data from Franklin County” (May 2024)
46. **KY** Malwarebytes, “Norton Healthcare attack exposes data on 2.5 million people” (May 2023)
47. **KY** Comparitech, “Ransomware shuts Jefferson County Clerk's offices for a week” (Jul 2024)
48. **LA** WAFB, “MOVEit breach exposes records of nearly every Louisiana driver” (Jun 2023)
49. **LA** The 74, “Medusa leaks St. Landry Parish schools data; families never notified” (Jul 2023)
50. **ME** Cybersecurity Dive, “MOVEit breach hits roughly the entire population of Maine” (May 2023)
51. **ME** SecurityWeek, “Central Maine Healthcare breach exposes 145,381 patients” (Jun 2025)
52. **ME** Bangor Daily News, “Cyberattack forces Bar Harbor offline, water plant controls cut” (Jul 2025)
53. **MD** BleepingComputer, “Ransomware at Frederick Health exposes 934,326 patients” (Jan 2025)
54. **MD** The Record, “Anne Arundel County confirms breach as Rhysida demands $2 million” (Oct 2026)
55. **MA** SecurityWeek, “Harvard Pilgrim ransomware attack exposes 2.86 million people” (Apr 2023)
56. **MA** WJAR (NBC 10), “Attleboro intrusion may have exposed SSNs and medical data” (Nov 2025)
57. **MI** SecurityWeek, “McLaren Health Care breach exposes 2.2 million people” (Aug 2023)
58. **MI** Comparitech, “Ransomware gang hits Michigan county on Election Day” (Nov 2024)
59. **MN** The Record, “Medusa leaks Minneapolis schools data after $1M demand” (Feb 2023)
60. **MN** FOX 9, “MOVEit hack exposes data on 95,000 Minnesota foster care students” (May 2023)
61. **MS** Security Affairs, “Rhysida attack on Singing River Health System hits 895,204” (Aug 2023)
62. **MO** The Record, “MOVEit breach via IBM exposes Missouri Medicaid data” (Jun 2023)
63. **MO** Fierce Healthcare, “Ascension ransomware attack exposes data of 5.6 million people” (May 2024)
64. **MT** Comparitech, “Anaconda hospital breach exposes SSNs and medical data of 21,000” (Aug 2024)
65. **NE** Nebraska Examiner, “Change Healthcare ransomware reaches 575,000+ Nebraskans” (Feb 2024)
66. **NE** Government Technology, “North Platte and Lincoln County, Neb., knocked offline” (Oct 2026)
67. **NV** Maine Attorney General, “Caesars hack exposes loyalty members' driver's license data” (Sep 2023)
68. **NV** News 3 Las Vegas (KSNV), “Unauthorized party breaches Clark County schools email system” (Oct 2023)
69. **NH** DataBreaches.net, “Vendor hack exposes SSNs of nearly 68,000 Concord Orthopaedics patients” (Nov 2024)
70. **NJ** SecurityWeek, “Prudential breach exposes data of 2.5 million people” (Feb 2024)
71. **NM** SecurityWeek, “Law firm breach exposes 300,000 Presbyterian Healthcare patients” (May 2024)
72. **NY** The Record, “BlackCat ransomware cripples Suffolk County government” (Sep 2022)
73. **NY** Chalkbeat, “MOVEit hack exposes data of 45,000 NYC students” (Jun 2023)
74. **NC** TEISS, “Phishing attack on Atrium Health exposes 586,000 people” (Apr 2024)
75. **ND** The HIPAA Journal, “Network intrusion at Dakota Eye Institute exposes 107,000 patients” (Oct 2023)
76. **OH** Security Affairs, “Ohio Lottery ransomware attack exposes SSNs of 539,000” (Dec 2023)
77. **OH** Infosecurity Magazine, “Rhysida ransomware exposes data of 500,000 Columbus residents” (Jul 2024)
78. **OK** Route Fifty, “Tulsa ransomware shuts city services, leaks 18,000 files” (May 2021)
79. **OK** Becker's Hospital Review, “Integris Health breach hits 2.4 million; patients get extortion emails” (Nov 2023)
80. **OR** BleepingComputer, “Phishing exposes data of 645,000 Oregon DHS clients” (Jan 2019)
81. **OR** Ashland.news, “MOVEit hack at Medicaid contractor exposes 1.7M Oregon Health Plan members” (May 2023)
82. **OR** Oregon DOT (official notice), “MOVEit hack exposes 3.5M Oregon driver's license records” (Jun 2023)
83. **PA** SecurityWeek, “BlackCat ransomware steals patient records and photos from LVHN” (Feb 2023)
84. **RI** The HIPAA Journal, “Human services agency breach exposes 115,000 Rhode Islanders' records” (Jul 2024)
85. **RI** Rhode Island Current, “Brain Cipher breach of RIBridges benefits system exposes 644,000 people” (Dec 2024)
86. **SC** The HIPAA Journal, “Rural Health Services breach exposes 36,500 patients' SSNs and records” (Feb 2025)
87. **SD** Becker's Hospital Review, “Imaging vendor breach exposes 21,000 Sanford Health patients” (Apr 2023)
88. **TN** SiliconANGLE, “HCA Healthcare breach exposes data of 11 million patients” (Jul 2023)
89. **TX** Texas Department of Transportation, “Compromised TxDOT account used to download 300,000 crash reports” (May 2025)
90. **UT** BleepingComputer, “University of Utah pays $457,000 after ransomware attack” (Jul 2020)
91. **UT** Comparitech, “Interlock ransomware steals Box Elder County data, 81,664 notified” (Aug 2025)
92. **VT** Vermont Public, “Joblink breach puts unemployment filers' SSNs at risk” (Mar 2017)
93. **VT** WCAX, “Slate Valley school district refuses ransom after data breach” (Oct 2026)
94. **VA** AuntMinnie, “Radiology Associates of Richmond hack affects 1.4 million patients” (Apr 2024)
95. **WA** Northwest Public Broadcasting, “Accellion breach may expose 1.6M Washington jobless claims” (Feb 2021)
96. **WA** Security Affairs, “T-Mobile API abuse exposes 37 million customer accounts” (Jan 2023)

97. **WA** SecurityWeek, “Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people” (Aug 2024)
98. **WV** The Record, “Cyberattack cancels classes for 20,000 Berkeley County students” (Feb 2023)
99. **WV** TEISS, “Phishing breach at CAMC exposes 67,000 patients' SSNs” (Oct 2024)
100. **WI** The HIPAA Journal, “Partner email hack exposes data of 19,000 Wisconsin Medicaid recipients” (Jun 2024)
101. **WI** The Record, “Chort ransomware steals data on 67,000 Sheboygan residents” (Oct 2024)
102. **WY** Wyoming Department of Health, “Wyoming health test data posted to public GitHub” (Apr 2021)
103. **WY** Wyoming Public Media, “Court vendor breach exposes Wyoming court users' personal data” (Sep 2026)