

Has my data been breached in 2024?

By: [Dieter Holger](#)

Edited by: [Jill Castellano](#)

 Updated 30 May 2024

Published: 30 May 2024

Data breaches are on track for a record year in 2024 as cybercriminals increasingly hunt for valuable information.

On average, a data breach exposing sensitive information, such as Social Security numbers, has around 172,000 victims, according to a ConsumerAffairs analysis of the Identity Theft Resource Center's database from 2018 to the first quarter of 2024. These breaches cause headaches for consumers, who then need to check if their information is secure elsewhere because they are now more vulnerable to [identity theft scams](#).

In the first quarter of 2024 there were 841 publicly reported data breaches, nearly doubling from a year ago, according to the Identity Theft Resource Center, a nonprofit that researches and advocates on identity theft issues. Previous years of data show the numbers trend higher later in the calendar year, suggesting 2024's final count may beat last year's record of 3,203 data breaches, up from the previous record of 1,860 in 2021.

"If we stay on the same path, we will break the record again," said the ITRC's chief operating officer, James Lee.



KEY INSIGHTS

Hospitality, financial services and health care companies are the leading industries for data breach victims who have their sensitive records exposed.

↓ [Jump to insight](#)

The vast majority of cyberattacks that lead to data breaches are going unreported, privacy experts say.

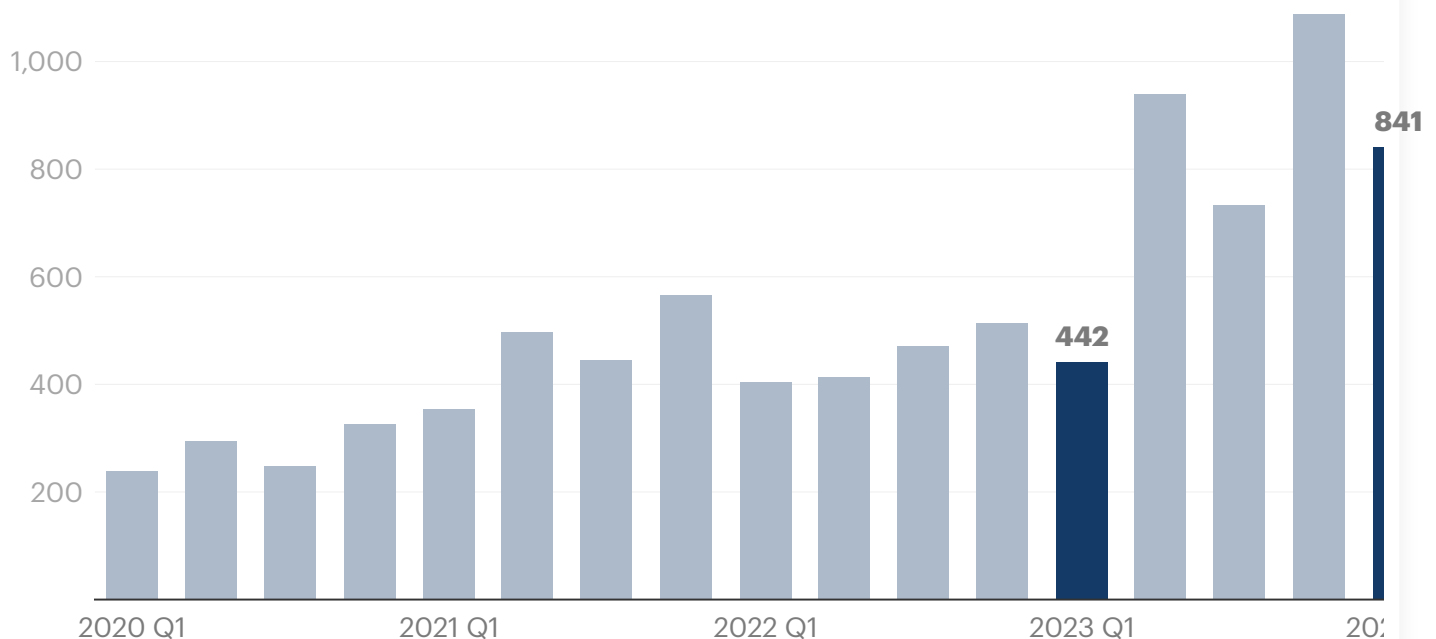
↓ [Jump to insight](#)

Vulnerabilities in the cloud, so-called vendor exploitation and new kinds of ransomware are making data breaches more threatening.

↓ [Jump to insight](#)

Data breaches by quarter

The number of data breaches nearly doubled in the first quarter of 2024 from a year prior



Note: Data covers single events and excludes attacks that compromised multiple companies at once.

Source: [Identity Theft Resource Center](#) • [Download image](#)



The largest data breach in the beginning of 2024 was at mortgage lender LoanDepot, exposing nearly 17 million victims. This is the company's second data breach since 2018, bringing its total to around 33.5 million victims who had sensitive information exposed.

LoanDepot declined to comment. In January, the company said it was investigating the incident and would offer credit monitoring and identity theft protection services for free to victims.

In the first quarter of 2024, financial services such as LoanDepot overtook health care as the industry with the most breaches, reaching 224 notices and surpassing the 124 notices from health care organizations.

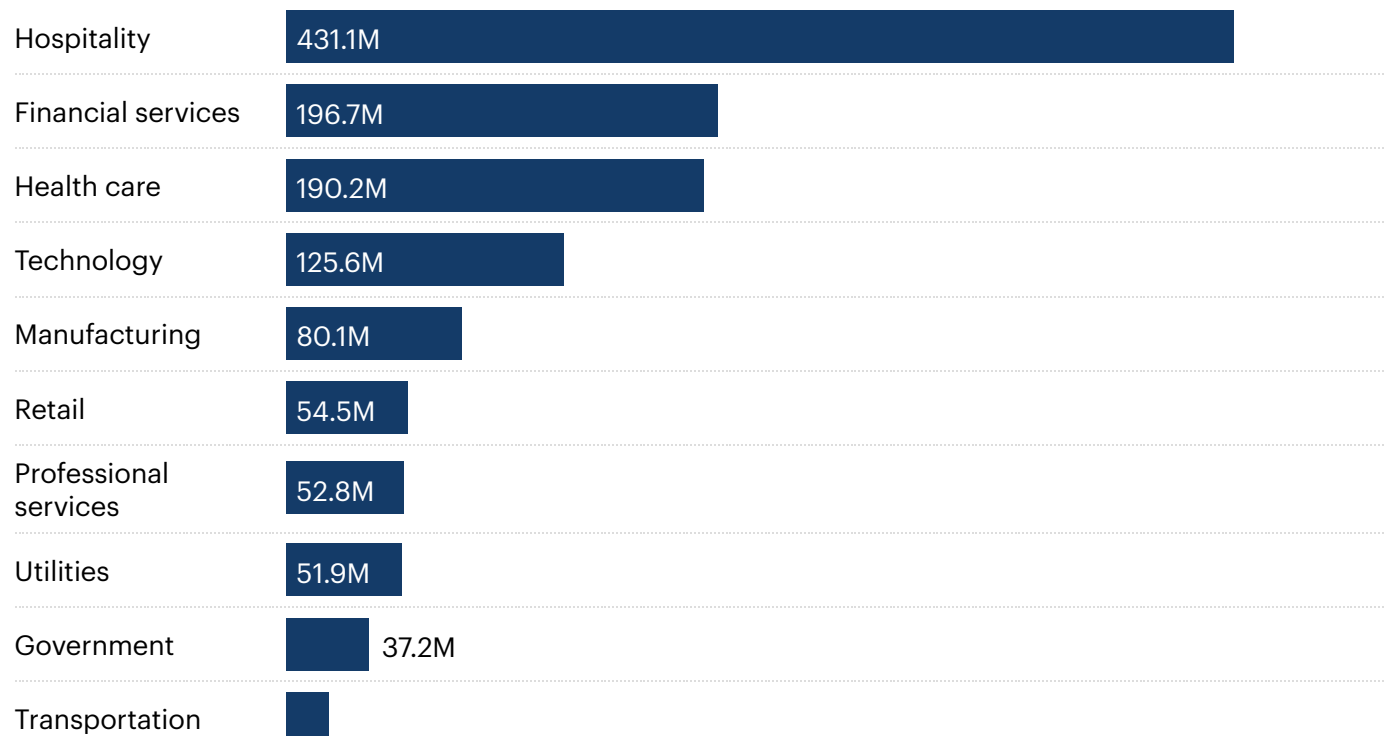
Since 2018, hospitality has pulled far ahead of other industries because of a massive breach Marriott reported in November of that year that stole up to 383 million guest records, although the company later said “the number of payment cards and passport numbers involved is a relatively small percentage of the overall total records involved.”

Financial services and health care organizations are closely ranked, with around 197 million and 190 million victims, respectively, followed by the technology sector, with around 126 million victims.

“It’s no surprise that financial services companies are frequent targets of bad actors because of the role the industry plays in most people’s lives,” the ITRC’s Lee said. “The same for health care companies.”

“Seeing such a large number of victims in the hospitality industry, though, is a reflection that hotels, airlines and entertainment companies like casinos handle massive amounts of personal information, which makes them a target,” he said.

Data breach victims with sensitive records exposed by sector



Note: Data from 2018 to the first quarter of 2024. Includes third-party attacks that hit multiple companies, but only represents publicly reported breaches that disclose how many individuals were affected. Figures can represent the upper limit of victims and not all victims necessarily had sensitive records stolen.

Source: Identity Theft Resource Center • [Download image](#)

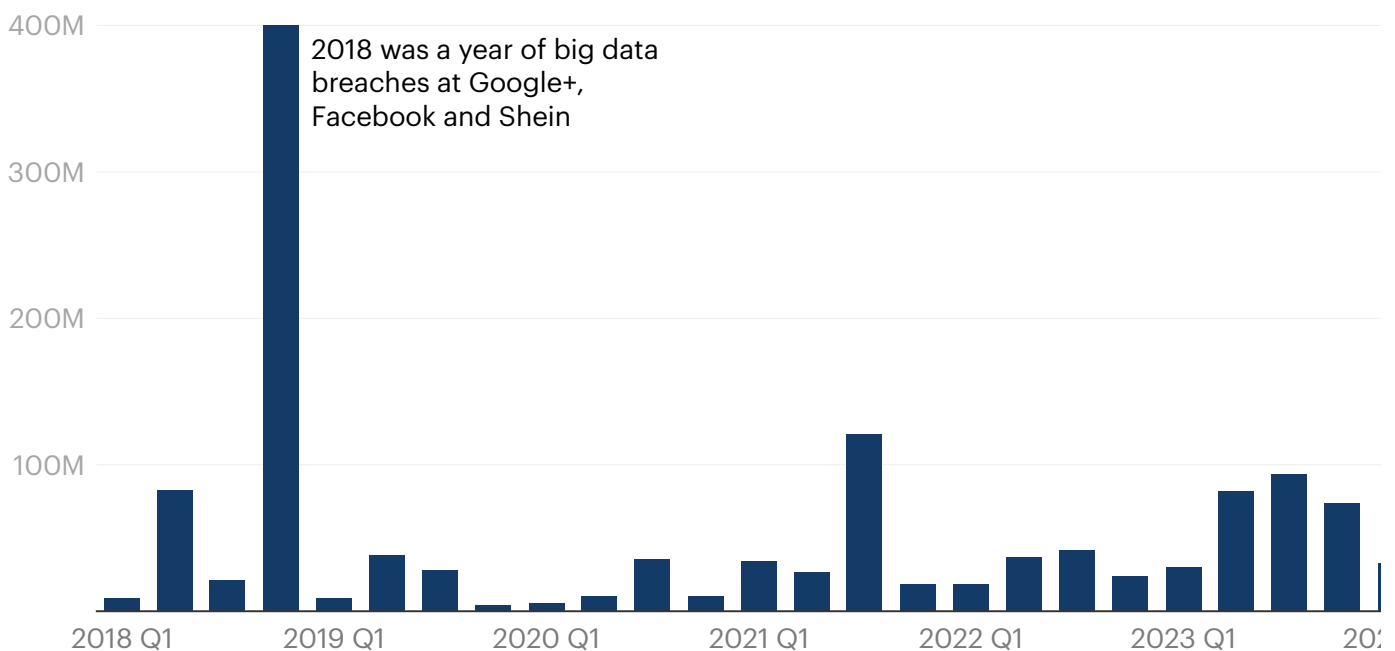


Even so, the number of victims is falling as the number of successful attacks rises. Privacy experts say this is because criminals are launching more targeted assaults for specific kinds of valuable information, instead of grabbing as much data as possible.

“The bad guys are impacting fewer individuals,” Lee said. “They’re doing that on a broader basis, so aggregated together the total number of (breaches) is higher.”

Data breach victims by quarter

Victims whose sensitive information, such as passwords and financial details, was exposed in a data breach



Note: Data from 2018 to the first quarter of 2024. Includes when breaches are reported and third-party attacks that hit multiple companies, but only represents publicly reported breaches that disclose how many individuals were affected.

Source: Identity Theft Resource Center



Not enough data on data breaches

The rise in data breaches comes as the Federal Trade Commission expanded reporting requirements so that nonbanking financial institutions like mortgage brokers and vehicle dealerships must have security programs in place to keep customer information safe. Privacy experts say the FTC rule should give a better picture of when and where data breaches are happening.

The public has a poor idea of how many data breaches are taking place in part because companies can be unaware of a cyberattack for months. Companies are also reporting under a patchwork of state requirements that vary on how quickly and detailed their disclosures need to be, compared with stricter nationwide laws in Europe, said Stuart Madnick, a professor of information technology at the MIT Sloan School of Management.

At recent talks with dozens of cybersecurity professionals, Madnick said no one raised their hand when asked if they thought one-quarter of cyberattacks were getting reported. Most hands went up when he asked if they thought 1% or fewer of cyberattacks were reported. Cyberattacks are by far the leading cause of data breaches.

“We don’t know what we don’t know,” Madnick said.

An FTC spokesperson said the rule requiring nonbanking financial institutions to report data breaches impacting 500 or more people within 30 days of discovery of a breach will help the agency gain better knowledge.

“We are hopeful this requirement will motivate companies to do more to implement appropriate safeguards to take steps to protect consumer data,” the spokesperson said.

While the FTC’s rule will encourage companies to protect their data a little more than before, it falls short, said Matthew Richardson, a partner at the law firm Brown Rudnick. By contrast, he said, the European Union’s data protection rules require companies to disclose within three days, and some U.S. states require the breached organization to pay for credit monitoring for the victim.

“The (FTC) rule is still a long way away from actually protecting anyone,” he said.

Where data breaches happen

Maryland leads the U.S. in number of victims of data breaches exposing sensitive information, with almost 390 million victims since 2018, an analysis of the ITRC’s data shows. That accounts for 30% of all victims over that time period.

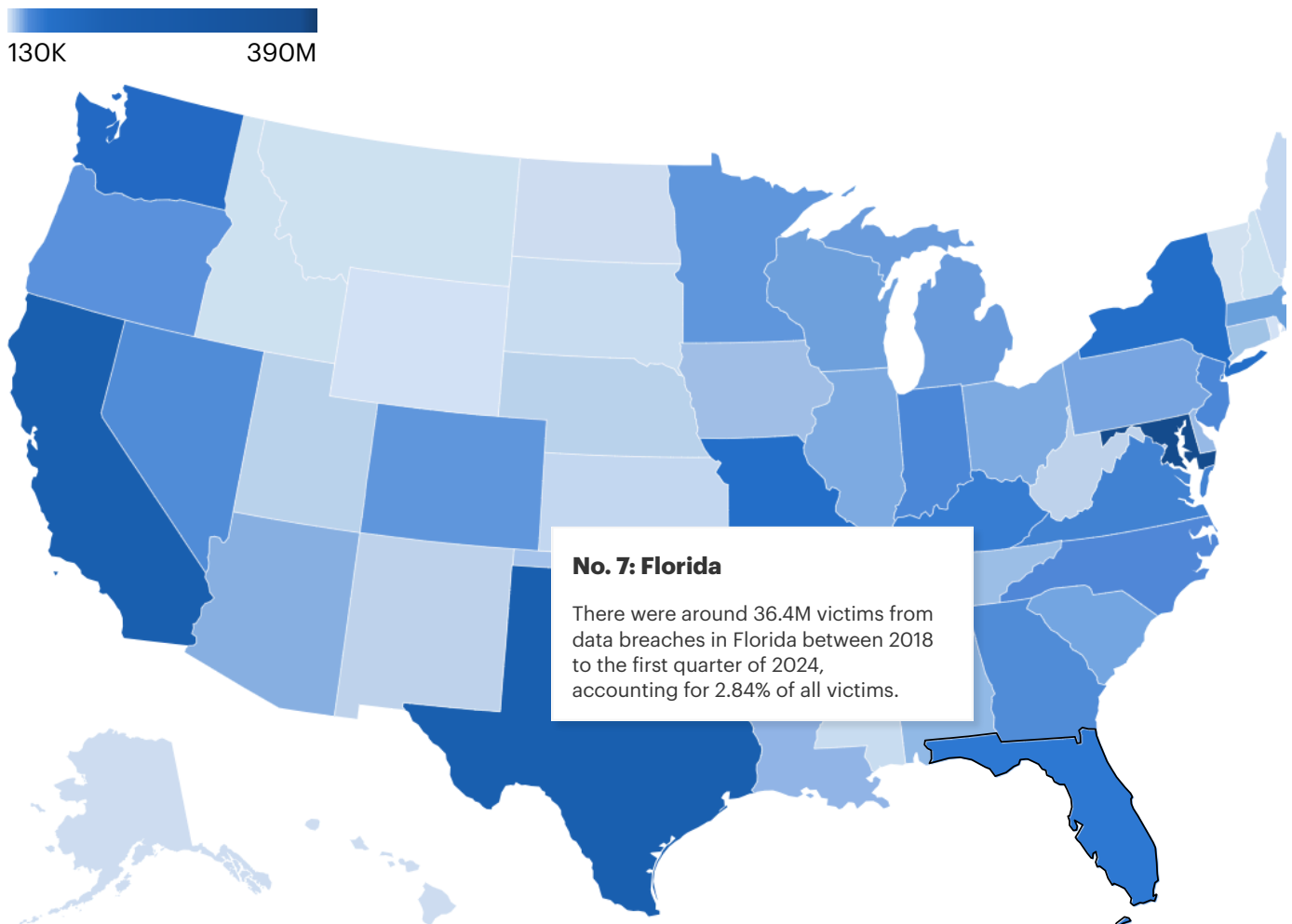
Texas comes in second place with around 130 million victims, and California ranks as a close third. Depending on reporting laws, state counts can be based on the organization's headquarters location or if people living in that state had their information stolen.

The ITRC's Lee said Maryland and Texas are ranking high largely because many companies are based in those states or are in proximity to government agencies with lots of data. California ranking third comes as little surprise, considering the number of technology companies managing large swaths of data that are based there, he said.

Still, more uniform reporting requirements are needed to understand the geographic scope of data breaches and their victims, Lee said. "It's difficult to develop a more accurate picture of where breach victims live," he said.

Victims of data breaches exposing sensitive information by U.S. state

Click a state to learn more



Note: Data as of 2018 to first quarter of 2024. States represent an organization's headquarters or, if specified, the location where an organization suffered a breach.

Source: Identity Theft Resource Center • [Download image](#)

More sophisticated threats

Data breaches are rising as new kinds of cyberattacks are emerging. Madnick of MIT said there are three such threats: the cloud, advanced ransomware and vendor exploitation.

The cloud. The cloud, where around 60% of corporate data is now held, is an area where companies often lack long-term experience in security, Madnick said. The National Security Agency has identified this phenomenon as so-called cloud misconfiguration, or when organizations install the cloud and don't realize there is a back door that hackers can access. Companies moving to the cloud quickly, without enough caution, is one of the main reasons data breaches are rising, Madnick said.

New ransomware. Traditional ransomware is used by cybercriminals to lock up a computer, scramble data and make someone or an organization pay to get the data unscrambled. Now, ransomware often makes a copy of private information, and cybercriminals threaten to publish it as blackmail, Madnick said. He added that ransomware criminals are acting like franchisees and creating teams of people using their software, which has dramatically increased the number of these attacks.

Vendor exploitation. As companies have gotten better at guarding their front door, cybercriminals are getting better at getting through a side door in a phenomenon called vendor exploitation, Madnick said. Cybercriminals are going after third parties that work with multiple companies and have keys to their data. He points to 2023's data breach stemming from file transfer service MOVEit, in which criminals were able to gain access to the U.S. Department of Energy, British Airways, pension funds and more.

Another factor is increasing the risk of falling victim to an attack: Cybercriminals no longer have to be that technically savvy. Instead, they can just buy the software and information they need on the dark web to carry out attacks against hubs of data, said cybersecurity firm Silverfort's chief information security officer, John Cunningham.

Cunningham said Silverfort's research shows that 65% of companies only protect some of their users with multifactor authentication, which makes it harder for hackers to break into accounts by creating extra password protection. What's more, with new technology, he said it can take as little as minutes for cybercriminals to crack passwords, when before it took months.

"There's still a lot of companies that aren't doing enough," Cunningham said.

Activity on the dark web shows cybercriminals continue to put value in Social Security numbers and other key personal information, said Chris Novak, managing director of Verizon Cybersecurity Consulting. Information being bought and sold is also expanding beyond Social Security numbers and health care data to information such as home equity and cryptocurrency wallets, he added.

“You can see the people who are stealing the data, then selling it to others,” Novak said. “We are going to continue to see that for the foreseeable future.”

Regulations on the way

New laws on data privacy are coming into force this year. In 2002, California was the first to pass a data breach notification law, and since then, all 50 states have followed.

More laws will go into effect soon in states such as Texas, Oregon and Montana, including rules that allow consumers to opt out of data collection.

New data privacy rules

Many new state laws enshrine a right to opt out of data collection, which can protect sensitive information from getting out

Authority	Name	Effective date	Details
Federal Trade Commission	Montana Consumer Data Privacy Act	May 13, 2024	Requires nonbanking institutions to report data breaches affecting 500 or more people.
Oregon	Oregon Consumer Privacy Act	July 1, 2024	Includes right to opt out of data collection, requires processing agreements of personal information, disclosures on how third-parties sell data and enforcement by attorney general.
Texas	Texas Data Privacy and Security Act	July 1, 2024	Includes expanded coverage of data processors, requires processing agreements of personal information

			and attorney general enforcement
Montana	Montana Consumer Data Privacy Act	Oct. 1, 2024	Includes right to opt out of data collection, requires processing agreements of personal information and attorney general enforcement.
Delaware	Delaware Personal Data Privacy Act	Jan. 1, 2025	Includes right for consumers to opt out of data collection, processing agreements of personal information and Delaware Department of Justice enforcement.
Iowa	Iowa Data Privacy Law	Jan. 1, 2025	Includes right for consumers to opt out of data collection, data processing agreements of personal information and attorney general enforcement
Tennessee	Tennessee Information Protection Act	July 1, 2025	Includes expanded privacy agreements, processing agreements of personal information and attorney general enforcement.
Indiana	Indiana Data Privacy Law	Jan. 1, 2026	Includes right for consumers to opt out of data collection, processing agreements of personal information and attorney general enforcement.

Source: Stuart Madnick, Angelica Marotta, White & Case



Still, reporting requirements and laws that exist now don't tell the public when companies have experienced a breach with no data, including when companies pay cybercriminals to save their

data from getting published or sold, Silverfort's Cunningham said. Such a requirement would give consumers a better idea about how secure services are and allow comparisons.

"That's a big gap today," he said.

What would help address the gaps is passing federal privacy legislation that requires notifications, but that process has been extremely difficult, said Emory Roane, policy counsel at the nonprofit Privacy Rights Clearinghouse, which co-sponsored and pushed for the passage of the California Delete Act. The law, which went into effect in January 2024, grants Californians the right to request to have their personal information erased from data brokers.

There is currently a bipartisan bill in Congress called the American Privacy Rights Act, but some experts are worried it would prevent states from passing stronger privacy laws, Roane said.

How to check if a web service is secure

While people should read privacy agreements, most people don't read these lengthy and sometimes confusing texts. Instead, privacy experts say there are some signs you can look for to see if companies have good protections in place.


Remember, if a company doesn't have your sensitive information, then it can't be exposed. A good starting point is to question why the company needs that information and ask yourself if you're comfortable giving it out.

- **Strong passwords:** Check if the service is requiring long and complex passwords.
- **Two-factor authentication:** This will require two or more credentials to log in to an account, such as both your password and a one-time code texted to your phone.
- **CAPTCHA:** If companies require a user to enter a series of characters from an image to use services, this will slow down attackers.
- **Read news:** A simple Google search can show if a company has been breached in recent years.
- **Security certifications:** Look for seals of approval, such as from the International Organization for Standardization, that a website follows best cybersecurity practices.
- **Encryption:** Check if a website uses encryption, such as SSL and the lock for HTTPS.
- **Passkeys:** There is a push to switch to passkeys, which authenticate logins without using a username or password.

What to do after a data breach

In the unfortunate event that you're notified of a data breach, there are some key steps that privacy experts say you should take to prevent identity theft.

- **Follow the letter:** Companies should send out a letter if you are a victim of a data breach. Read it carefully to get more details about what data was exposed and the steps the company recommends you take.
- **Freeze your credit:** Contact each of the three credit bureaus, Experian, Equifax and TransUnion, and get your credit frozen so a criminal can't open cards or other lines in your name.
- **Credit monitoring:** Sometimes, companies will offer free credit monitoring or other services after a data breach.
- **Reset passwords:** Change your passwords and use different ones for services.
- **Use a password manager:** LastPass and services built into web browsers such as Google Chrome and Microsoft Edge can create and store strong passwords for you.
- **Opt out of data collection:** If you have the right in your state, you can email services you use to request they don't collect your data for the use by third parties.
- **Request to have your data deleted:** For services you don't use, ask to have your data deleted. California and other states have written this into law.

 [Home](#) > [Best Identity Theft Protection](#)