Caltech

What To Do If Your Data Has Been Breached

From time to time, you may see news about data breaches. A data breach occurs when personal information such as your Social Security number, financial data, medical information, or login credentials is exposed or accessed without authorization.

Even if you're not directly impacted, consider basic precautions like using strong, unique passwords, enabling multi-factor authentication, staying alert to phishing, and reviewing your financial/credit activity. Below are FAQs and resources to learn about data breaches and options to protect yourself.

Frequently Asked Questions (FAQs)

Q: What is a data breach and how might it affect me?

A: A data breach is unauthorized access to personal information - for example, contact details, date of birth, SSN, government IDs, etc. Exposure doesn't always lead to misuse but can increase the risk of identity theft or fraud.

Q: What signs of identity theft should I watch for?

A: Be alert to unfamiliar accounts, charges, hard inquiries, or official notices that don't match your activity.

Q: I received a notice regarding a data breach of my information. What should I do?

A: You should consider:

- Enrolling in complimentary credit monitoring offered by the sender.
- Placing a fraud alert and/or a credit freeze and reviewing your credit reports.
- If you notice misuse, you can report it and get a personalized recovery plan at IdentityTheft.gov.

Q: Should I freeze my credit even if I haven't received a data breach notice or seen fraud?

A: A credit freeze is a strong preventive measure and is recommended by federal guidance, especially where SSNs may be exposed; you can temporarily lift it when needed.

You may freeze your credit by contacting Equifax, Experian, and TransUnion online or by phone. Freezes and alerts are free; freezes stay in place until you lift them, while initial fraud alerts last one year and can be renewed. Step-by-step instructions are available from USA.gov and FTC.gov.

Caltech

Caltech Resources

ComPsych EAP: Benefit-eligible employees get no-cost, confidential, 24/7 telephonic legal and financial information through CompPsych. Eligible employees can also request local attorney referrals (including a free 30-minute consultation and a 25% discount), access articles and checklists, receive breach/scam alerts, or call anytime for help and support (e.g., disputing fraud, credit recovery).

IDShield**:** Enrolled employees have access to full-service identity restoration - including fraud alerts, disputes with creditors/credit bureaus, and limited power of attorney when needed - plus 24/7 emergency help, tri-bureau credit/dark web/public records monitoring with alerts, and a $3M Identity Fraud Protection Plan that reimburses covered expenses and losses.

Caltech Benefits Team: Visit MyBenefits.caltech.edu or email hrbenefits@caltech.edu for additional information.

Additional Resources

The Federal Trade Commission has additional information and resources, including videos on What To Do After a Data Breach and how IdentityTheft.gov Helps You Report and Recover from Identity Theft.

The IRS also has information on what you should know and do about data breaches.