What is a Data Breach?

What to do in case you become a victim

When a company's records are lost or stolen, your sensitive information (like your Social Security number or bank account information) can land in the hands of an identity thief. The thief then can use your information to siphon money from your bank account, gain access to your credit cards, or to create new accounts in your name.

As a result, your credit reports can be blemished with unpaid accounts and you can start receiving phone calls from collection agencies. Data breaches can happen at any type of business, whether it's a local dental clinic or a big online retailer.

What you should know:

1. State laws typically require the business to notify affected customers within a certain amount of time or be subject to a fine.

2. The District of Columbia, Puerto Rico, and the Virgin Islands all have some type of data breach law. Five states—Alabama, Kentucky, Mississippi, New Mexico, and Colorado—do not.

3. In the past, some companies have paid for 6 to 12 months of credit monitoring for affected individuals. While this is something the Federal Trade Commission (FTC) recommends to businesses that have suffered a data breach, it isn't a requirement.

What to do if you are a victim of a data breach:

If you think you've been the victim of identity theft, here are some tips to help you resolve the matter.

Step 1: Contact one of the three credit bureaus

- By contacting one of the three reporting agencies or credit bureaus (Experian®, TransUnion®, or Equifax®), an initial security alert (or fraud alert) can be immediately included in your credit profile to inform creditors to check your identity before approving credit. Just remember, an alert may limit your chances of being approved for new credit right away or you may be asked to provide additional proof of identification.
- Securing a report from each of the three bureaus is highly recommended if you believe you might be the victim of identity theft or fraud. When you contact a credit bureau regarding your case, you may also request a complimentary credit report. If you alert one of the credit reporting bureaus about the fraudulent activity, the alert will be shared with the other credit reporting companies, so they can update their credit files.
- Be sure to keep a record of all phone calls and all documents in connection with resolving this matter in case you need to refer to these items later.

Step 2: Review credit report(s) carefully

- Thoroughly review your credit report for suspicious information or activity. Request a copy of your credit report from the credit bureaus. You should also review your billing statements and immediately notify each creditor to dispute what you believe are fraudulent charges. Keep detailed records of your conversations and interactions.
- If you've identified fraudulent data, keep a list of all the potentially fraudulent information found on your credit report. Any data included that looks unfamiliar, including accounts, credit lines, addresses, and names should be reported.

Step 3: Obtain an Identity Theft Report

- An Identity Theft Report will help you get fraudulent information removed from your credit report(s), prevent companies from collecting debts that result from identity theft, and can place an extended fraud alert on your credit profile. An extended fraud alert will last for seven years.
- To create an Identity Theft Report, fill out a complaint form on the Federal Trade Commission's website and print the Identity Theft Affidavit. Use that to file a police report and create your Identity Theft Report. You can also obtain an identity theft report by filing an official report about the identity theft to a federal, state, or other local law enforcement agency.

Step 4: Obtain an extended fraud alert and request removal of fraudulent data from your credit report

After you've obtained an Identity Theft Report, contact one of the bureaus again to place an extended fraud alert on your credit profile and have the fraudulent information removed.

There are four pieces of information that a credit bureau needs to remove fraudulent activity on a credit report:

- Proof of your identity
- Identification of fraudulent data from your credit report
- A copy of an official identity theft report (refer to Step 3)
- A statement from you that the fraudulent activity does not relate to any transaction made by you

Once a bureau has received the required information, that bureau will remove all fraudulent activity from your credit report within four business days.

After following these steps, it's important to continue monitoring your credit history regularly. Understanding how identity theft can be detected early and resolved is one of the best things you can do to help protect yourself from the harmful effects of identity theft and identity fraud.

If you are a victim identity theft or suspect you may be a victim due to a data breach, you have first-hand knowledge of the stress it can cause.
