IDT911
CLIENT | ALERT

HOW TO PROTECT YOURSELF AFTER ANTHEM'S DATA BREACH

Identity thieves can do a lot of damage with the treasure trove of sensitive information stolen in the Anthem data breach.

The stolen data included the names, addresses, Social Security numbers (SSNs), birth dates, and email and employment information for 80 million current and former customers and Anthem employees.

Identity thieves can use the stolen information to:

- File and steal tax refunds
- Open new credit cards
- Secure a loan
- Apply for a job
- Pursue medical treatment

How victims protect themselves

1. **Place a fraud alert on their credit file.** An alert placed with one of the three major credit bureaus signals to potential creditors that you could be a victim of identity theft. Initial Fraud Alerts last for 90 days and require potential creditors to confirm the legitimacy of your identity before granting credit. Extended Fraud Alerts last for seven years.
2. **Review credit reports for any unusual activity.** Visit annualcreditreport.com, the government-mandated source for free annual credit reports. Investigate suspicious activity and monitor it until it's resolved. Also, look for signs of fraud in your medical files, on your Social Security statement, in insurance claims, and in public records.
3. **Consider placing a security freeze on their credit report.** This may be necessary if you're experiencing fraud as a result of the data breach. A freeze locks access to your credit, so no one will be able to open a new account in your name.