# What happened?

On Sept. 7, Equifax confirmed they had suffered a major data breach, in which criminals accessed consumer files and personal information of around 143 million Americans. The Equifax data breach was executed through a “website application vulnerability.”

# Scope of Breach

When the Equifax data breach was initially discovered on July 29, the company responded by hiring an independent security firm to promptly begin investigating.  Names, Social Security numbers, birthdates and addresses were among the exposed information. Some driver’s licenses were also compromised.

The investigation also found that credit card information of 209,000 U.S. consumers, and sensitive documents belonging to 182,000 U.S. consumers were also exposed. However, Equifax’s core consumer and commercial credit reporting databases were not affected.

Equifax is offering all U.S. consumers free credit and Internet monitoring services for a year. If you already have monitoring services through EZShield, be sure that your information is stored in your Online Identity Vault™, and that your monitoring alerts are turned on. This will help alert you to any malicious use of personal information stolen in the Equifax data breach.

# What should I do?

## Next Steps:

1. Visit **equifaxsecurity2017.com** and follow the instructions on the site to determine whether your information was exposed. If Equifax indicates that your information could have been affected by the breach, place a credit freeze or fraud alert on your files from all three credit bureaus.

2. Continue monitoring your financial accounts and credit reports for suspicious activity that could mean fraud or identity theft.

## Other Protective Measures to Consider:

1. Visit your Online Dashboard to securely store your personal information, Social Security number, credit and debit cards. For customers who have monitoring services, keep your eyes peeled for any related alerts.
2. If you don't have Internet or Credit Monitoring services on your dashboard, consider adding them or take advantage of Equifax's free one-year identity theft protection services.
3. Call the Resolution Center if you have any questions, or you think your information was exposed.

---

## The Importance of Monitoring Services

**Internet Monitoring:** When your information is exposed in a breach, it is often then sold by criminals online. Internet Monitoring will alert you if your information is found being traded on the Dark Web — allowing you to cancel a card or close an account before more substantial damage is done.

**Credit Monitoring:** The Equifax data breach is especially concerning because the exposed information includes Social Security numbers. Criminals can then use this information to open new accounts or new lines of credit under your name. Credit Monitoring will alert you of any inquiries or changes to your credit report.

---

Continue following Fighting Identity Crimes to stay up-to-date on the latest data breaches and scams, as well as tips from our industry experts on how to secure your identity.