STATE OF NEW MEXICO
OFFICE OF THE ATTORNEY GENERAL

Equifax Data Breach Consumer Information

Why is Equifax unique among data breaches?

This data breach is unique in that consumers may not be aware that Equifax has their personal information. In other types of data breaches like those from credit card application information at other companies, consumers have knowingly released their information. This case is different because consumers do not directly or voluntarily give their information to Equifax. Equifax's consumer information comes from a number of different sources, including credit card companies and many other companies that participate in the credit reporting process. **Given the massive scope of this data breach, it is important for all New Mexicans to check whether their personal information has been exposed and take all steps to protect themselves.**

Tips for protecting yourself if you think your personal information has been compromised in a data breach:

- **Find out if your information has been compromised:**

https://www.equifaxsecurity2017.com/potential-impact/ .

Equifax has set up a website with general information about the breach, which can be found here:
https://www.equifaxsecurity2017.com/.

If you choose to participate in Equifax's free credit monitoring for directly impacted consumers, **be absolutely sure to read the fine print carefully, you may be agreeing to terms that limit your rights.**

- **Watch your bank account and credit cards:** Be diligent. Carefully check all bank accounts and credit card statements on a regular basis. It's important to not just watch them now, while this is in the news, but to watch them months from now, since the criminals who took the information may be very patient and wait until consumers have forgotten about the issue to act.

- **Report any suspicious activity** to your bank or credit card company right away. Any delay in reporting fraudulent activity may make it harder for you to get that money back.

- **Check for new credit accounts that you did not open:** This is just as important as watching the accounts you know about. Sometimes, identity theft isn't limited to the bank and credit accounts you have opened yourself. Data thieves may use your information to open new accounts in your name. A good credit monitoring service can help you do this on a weekly, monthly or quarterly basis. If you choose not to use a credit monitoring service, you can check your credit report for free once a year. Be sure to immediately dispute any inaccurate information.

- **Freeze your credit report:** If you are not planning on applying for credit (e.g. buying a house, a car or applying for a credit card), another option is to put a credit freeze on your credit report. A credit freeze restricts access to your credit report, meaning that most companies who request your credit report will not be able to access it. If your credit report is frozen, thieves who apply for credit in your name will have a much harder time opening new accounts. However, placing such a freeze should be considered carefully, since the lead time needed to unfreeze it may be significant. The FTC website is a great resource for more information on freezing your credit reports:
  https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

- **Put a fraud alert on your credit reports:** You can ask any one of the three credit reporting agencies to put an initial fraud alert on your credit reports. The agency you ask must share your request with the other two agencies. When you have an alert on your credit report, the company must verify your identity before extending credit, which means if a data thief attempts to open a new account in your name, the credit company may try to contact you. Initial alerts are good for 90 days and may be renewed. If you are an active duty member of our military, you may place a 1 year renewable alert on your credit. For more information go here:
  https://www.consumer.ftc.gov/articles/0275-place-fraud-alert
  or here: https://www.consumer.ftc.gov/articles/0273-active-duty-alerts

For more information on identity theft or on what to do when your personal information is stolen go here:

What to do after a data breach:
https://www.consumer.ftc.gov/media/video-0127-what-do-after-data-breach

Tips for when your personal identifying information is missing or stolen:
https://www.identitytheft.gov/Info-Lost-or-Stolen

Recovering from identity theft:
https://www.consumer.ftc.gov/features/feature-0014-identity-theft

FTC on the Equifax data breach:
https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do?utm_source=govdelivery