



**ATTORNEY GENERAL STEVE MARSHALL AMONG 32 ATTORNEYS GENERAL
CALLING ON EQUIFAX TO STOP CHARGING FOR CREDIT MONITORING
AND TO REIMBURSE FEES CONSUMERS PAY FOR SECURITY FREEZES TO
THEIR ACCOUNTS AS A RESULT OF EQUIFAX'S MASSIVE DATA BREACH**

***AG MARSHALL ALSO WARNS CONSUMERS AGAINST FALLING VICTIM TO SCAMMERS
CLAIMING TO BE FROM EQUIFAX***

(MONTGOMERY) – Alabama Attorney General Steve Marshall is among 32 attorneys general calling on Equifax to drop fees it charges for its credit monitoring service and to reimburse consumers who were forced to pay for security freezes to their credit accounts as a result of the Equifax data breach.

“By Equifax’s own admission, the company suffered a massive data breach potentially compromising the credit of 143 million people,” said Attorney General Marshall. “While my office and those of many of my fellow attorneys general prepare to investigate the circumstances of this unprecedented data breach, it is important that Equifax stop efforts to profit off of the very same people who were victim of its own failure to protect their credit information.”

In their [letter to Equifax](#), Attorney General Marshall and the other attorneys general called on the credit management company to halt its fee-based services to consumers and to extend the period of signup for free credit monitoring until at least January 21, 2018.

“We object to Equifax seemingly using its own data breach as an opportunity to sell services to breach victims. Selling a fee-based product that competes with Equifax’s own free offer of credit monitoring services to victims of Equifax’s own data breach is unfair, particularly if consumers are not sure if their information was compromised. Equifax cannot reap benefits from confused consumers who are likely only visiting Equifax’s homepage because they are concerned about whether the breach affects them and their families.”

The attorneys general also voiced objection to consumers being forced to pay for security freezes to their credit accounts as they attempt to protect themselves from Equifax’s data breach.

“Although Equifax is not charging consumers a fee for its own security freeze service, these consumers are furious that they have been forced to pay for a security freeze with other

501 Washington Avenue • Montgomery, AL 36104 • (334) 242-7300

www.ago.alabama.gov



companies, such as Experian and TransUnion, when this privacy breach was no fault of their own. We agree with these consumers that it is indefensible that they be forced to pay fees to fully protect themselves from the fallout of Equifax's data breach. Accordingly, we believe Equifax should, at a minimum, be taking steps to reimburse consumers who incur fees to completely freeze their credit."

The attorneys general also asked Equifax to address complaints of long wait times or the inability of consumers to access its call center.

"...[I]t has been generally reported that consumers are encountering long wait times or are unable to get through to your call center. We have received similar complaints from our consumers, who have also stated they cannot locate Equifax's phone number on your website. We request that you feature your call center number more prominently on www.equifax.com and www.equifaxsecurity2017.com. In addition, this hotline should be available 24 hours a day and properly staffed to ensure shorter wait times."

Separately, Attorney General Marshall warned Alabamians to be on the lookout for scammers hoping to take advantage of consumers' concerns over the data breach.

"Although Equifax has informed attorneys general that it will not be emailing, texting or calling impacted consumers, the Federal Trade Commission is reporting that fraudsters are already attempting to cash in on the unsuspecting public through phone scams," said Attorney General Marshall. "I urge anyone who receives such a phone call, text or email to report it to the Alabama Attorney General's Office at **1-800-392-5658**."

Tips for Consumers to Avoid being Victimized:

- Don't give personal information. Don't provide any personal or financial information unless you've initiated the call and it's to a phone number you know is correct.
- Don't trust caller ID. Scammers can spoof their numbers so it looks like they are calling from a particular company, even when they're not.
- If you get a robocall, hang up. Don't press 1 to speak to a live operator or any other key to take your number off the list. If you respond by pressing any number, it will probably just lead to more robocalls.
- If you gave your personal information to an imposter, it's time to change any compromised passwords, account numbers or security questions.
- Verify your credit reports with all three credit bureaus, Equifax, TransUnion, and Experian, by visiting <https://www.annualcreditreport.com>.

- Monitor existing accounts closely. Check bank and credit card statements for unauthorized charges.

For more information about the Equifax breach, visit Equifax's website, www.equifaxsecurity2017.com, or contact their call center at 1-866-447-7559.