STATE OF ALABAMA
STATE BANKING DEPARTMENT

Kay Ivey
Governor

Mike Hill
Superintendent of Banks

STATEMENT CONCERNING BREACH OF CUSTOMER DATA AT EQUIFAX
September 13, 2017

Last week, Equifax, one of the three major credit reporting agencies, announced a security breach occurred from mid-May through July 2017 that potentially impacts 143 million consumers. We have been informed that the hackers obtained people's names, social security numbers, birth dates, addresses, and in some cases driver's license and credit card numbers. Also, personal identifying information was exposed for certain customers involved in credit report disputes. Equifax has set up a website for consumers to check if their information was exposed at www.equifaxsecurity2017.com. Click the "Potential Impact" tab, enter your last name and the last 6 digits of your social security number, and the website will let you know if you have been affected by the breach. Please make sure you are on a secure computer and use an encrypted network connection when entering your personal information.

Given the wide-spread nature of the Equifax breach, it is important that consumers pay close attention to their bank and credit card account statements as well as their credit reports. If you notice any unauthorized activity, it is recommended that you report it to your financial institution or credit provider immediately. A copy of your credit report may be requested online at www.annualcreditreport.com. You're entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting companies: Equifax, Experian, and TransUnion.

If you receive a notice or otherwise determine that your personal information may have been exposed in the Equifax breach, you can take the following steps to help protect yourself from identity theft:

- Consider whether you want to sign up for the free credit monitoring services that Equifax is offering.
- Consider placing a credit freeze on your files. A credit freeze makes it harder for someone to open a new account in your name. If you place a freeze, you'll have to lift the freeze before you apply for a new credit card or cell phone - or any service that requires a credit check. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- If you decide not to place a credit freeze, at least consider placing a fraud alert on your files. A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.

- Try to file your taxes early - before a scammer can. Tax Identity Theft happens when someone uses your Social Security number to get a tax refund or a job.
- Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt - even if they have part or all of your Social Security number, or they say they're from the IRS.

Additional information regarding steps you can take to protect yourself from identity theft if your personal information has been exposed in a data breach can be found at www.identitytheft.gov/Info-Lost-or-Stolen. Also, the Consumer Financial Protection Bureau has updated its website with details on identity theft protection following the Equifax breach at: www.consumerfinance.gov/about-us/blog/identity-theft-protection-following-equifax-data-breach/.

Sincerely,

Mike Hill

Mike Hill
Superintendent of Banks
Alabama State Banking Department