Texas Department of
Savings and Mortgage Lending

From: Caroline Jones, Commissioner
To: State Savings Bank Presidents and Chief Executive Officers

---

September 13, 2017

Equifax Breach Resources

As you might have already learned, on September 8th, Equifax, one of the major credit reporting agencies, announced a breach from mid-May through July 2017. During this period, hackers accessed people's names, social security numbers, birth dates, addresses, driver's license numbers, and credit card numbers.

State savings banks in Texas have maintained an extremely strong security posture; however, there remains a need to be constantly vigilant. The Conference of State Bank Supervisors (CSBS) has been in touch with FS-ISAC (Financial Services-Information Sharing and Analysis Center), which is monitoring the situation for new information, including indicators of compromise and TTPs (Trust Transfer Process) that can possibly assist financial institutions to enhance their own defenses.

Financial institutions can be proactive to mitigate the fallout from the Equifax and other breaches:

- **Patch Management** – Verify that all information technology and information security patches have been installed.
- **Confirm credit report information with your customers** – Before originating loans and before denying any loan, confirm credit report information with your customers.
- **Additional security measures –** If a customer informs a financial institution that they were one of the consumers whose information was stolen, the financial institution can code the customer account with a "red flag" to contact the customer at a pre-designated contact number or email prior to opening an account, applying for credit, or making any changes on existing accounts. The customer can also contact the major credit reporting bureaus to put a Fraud Alert on their account.

Equifax set up a website for consumers to check if their information was exposed: www.equifaxsecurity2017.com. This website has not been verified by regulators, but may provide pertinent information to consumers trying to determine whether they have been affected by the breach. To use the website, consumers should click the "Potential Impact" tab; enter their last name and the last 6 digits of their social security number. Consumers are urged to take standard precautions, including using a secure computer and an encrypted network connection.

The Federal Trade Commission released some steps to help protect consumers after a data breach:

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. Accounts or activity that you don't recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do.
- **Consider placing a** credit freeze **on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for charges you don't recognize.
- If you decide against a credit freeze, **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.
- **File your taxes early** — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.

Visit Identitytheft.gov/databreach to learn more about protecting yourself after a data breach.

Please contact your supervisory analyst for more information.

Please disseminate this information as you deem appropriate.

Caroline C. Jones
Commissioner