

## Equifax Data Breach Alert

On September 7, 2017, Equifax, one of the major credit reporting agencies, disclosed a data breach that potentially impacted 143 million U.S. consumers. Blackhawk Area Credit Union DOES NOT report to Equifax, however, we feel this information is valuable for our members.

Equifax is offering a free year of its credit monitoring service to consumers whose information was compromised. At this time, there are concerns about Equifax's credit monitoring service. Here are links for current information and concerns:

Krebs On Security:

<https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/>

Washington Post:

[https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm\\_term=.0fa760bc7eec](https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm_term=.0fa760bc7eec)

Equifax Website on the Data Breach:

<https://www.equifaxsecurity2017.com/>

### What You Can Do to Protect Yourself:

- Personal credit reports should be monitored for new applications that were filed on your behalf.
- Monitor all monthly statements for any unauthorized payments.
- Monitor your existing credit card and Credit Union/ bank accounts closely for charges you don't recognize; such as address or phone number changes.
- 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.
- 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. The IRS will only contact you through the mail.
- **NEVER** respond to an e-mail asking you to verify or update your personal information
- Never click on links in unsolicited e-mail that you receive
- Delete any unsolicited e-mails in your e-mail accounts; don't even open them!
- Protect your passwords. Never write them down or enter them online unless you initiated the transaction.
- Never give out your personal or financial information on the phone or online unless you initiated contact
- Check your credit report at least once annually or sign-up for weekly or monthly alerts through credit management agencies
- At home, use spam blockers, firewalls, virus protection, and adware & malware destroyers
- Update your Operating System whenever security patches are available