Reported Data Breach

According to Equifax, the breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. They also stole credit card numbers belonging to about 209,000 people and dispute documents with personal identifying information from about 182,000 people.

Equifax has established a website www.equifaxsecurity2017.com for customers to identify if their information was potentially compromised.

Here are some other steps to take to help protect yourself after a data breach:

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. **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.

You can visit the Federal Trades Commission's website www.identitytheft.gov/Info-Lost-or-Stolen to review additional options for consideration to protect against identity theft.