Equifax Inc., one of three nationwide credit reporting companies, announced a cybersecurity incident which potentially impacts approximately 143 million U.S. consumers. Attackers accessed personal data such as names, social security numbers, birth dates, addresses, drivers license numbers, credit card numbers, and other documentation with personal identifying information. The main Equifax website application that allows consumers to send documentation involving credit disputes and servers that hosted databases which stored customer feedback logs, were accessed through a weakness in the website. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.

The Gifford Sate Bank utilizes Equifax for credit reporting only for fixed rate mortgage loans through a third party, which encrypts all personal information. At this time,Equifax has found no evidence of unauthorized activity on their core consumer or commercial credit reporting databases, which third parties utilize to send and store customer information.

The Gifford State Bank is committed to keeping your personal information secure and will continue to monitor and update customers of any new information regarding the breach.

If you have utilized Equifax's website for any credit reporting or credit disputes, here are some ways to protect yourself:

-Equifax has set up a Web site — https://www.equifaxsecurity2017.com — that consumers can visit to see if they may be impacted by the breach. You can also call Equifax at 866-447-7559.

-The Equifax site also lets consumers enroll in TrustedID Premier, a 3-bureau credit monitoring service and ID theft monitoring service, for free, up to one year if customers sign up by November 21, 2017.

-Keep a close eye on your finances and monitor your account activity. The Gifford State Bank offers services such as Online Banking and a Mobile Banking App so you have access to your account 24/7.

-It's also important to check online accounts such as hotel and airline loyalty programs as hackers frequently slice and dice information from large data breaches, selling groups of user information for specific companies.

- Hackers often use news of big breaches to conduct "phishing" campaigns, sending official-looking emails that make it seem as if the affected company or other legitimate services are asking them to supply information or click through to a link to repair any damage. When in doubt, call or email the company that appears to be sending the message separately, do not go through the email you've been sent.

- If you have any further questions or concerns about your Gifford State Bank accounts feel free to contact us at 217-568-7311.