Equifax Breach

First Harrison Bank is aware of the data breach announced by Equifax. While First Harrison Bank in no way endorses the information provided by Equifax, we would like to let our customers know that In their announcement, Equifax included a website for consumers to obtain further information about the breach. That website can be found at https://www.equifaxsecurity2017.com/. In addition to the website, Equifax also announced that a special call center has been set up to answer questions; the number is 866-447-7559.

First Harrison Bank takes the privacy of its customers very seriously, and processes have been reviewed to ensure that any and all information we house is maintained in accordance with our privacy and business standards. Our processes will continue to be reviewed to ensure your information is protected.

All consumers should be diligent about reviewing all account statements and credit reports for fraudulent information and/or transactions, and if you believe you may be the victim of identity theft, there are steps you can take:

1. Contact the Identity Theft Hotline of the Federal Trade Commission (FTC) on the internet at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or call toll free 877-438-4338. The FTC places information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.

2. File a police report with local law enforcement agencies to document the crime.

3. Contact fraud departments of Equifax credit bureau at 888-766-0008, or Online at the Equifax Fraud Alert Website at help.equifax.com>home>alerts or www.alerts.equifax.com and request that a “90 Day fraud alert”, an “Automatic Fraud Alert”, or a “victim’s statement” be placed in the customer’s credit line. This alert places creditors on notice that the customer has been the victim of fraud and the victim’s statement asks creditors not to open additional accounts without first contacting the customer. You may also consider requesting the credit bureaus to “freeze” your credit report, thereby making it more difficult for an identity thief to obtain credit in your name. Equifax will contact TransUnion and Experian for you.

First Harrison Bank

Equal Housing Lender

MEMBER FDIC

- **Automatic Fraud Alerts vs Initial 90 Day Fraud Alert**
  - An initial 90 day fraud alert expires every 90 days so the customer has to remember to manually renew it if they want an initial 90 day fraud alert to remain on their credit file. Subscribers of eligible Equifax monitoring products enjoy free access to the Automatic Fraud Alert feature which addresses this by automatically renewing their Equifax initial 90 day fraud alert and requesting that TransUnion and Experian do the same.
- **Fraud Alerts Fee**
  - There is no fee for placing an initial 90 day fraud alert on the customer's credit file.
  - For the Automatic Fraud Alerts, the customer needs to contact Equifax to see if there are fees.
- **Credit Freeze**
  - Credit Freeze is known as a security freeze, this tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your file, they may not extend credit.
- **The Difference between a Credit Freeze and Fraud Alerts**
  - A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

4. Obtain a free credit report from the above listed credit bureaus or at www.annualcreditreport.com . The credit bureaus must provide a free credit report if the customer believes the report is inaccurate due to fraud.
   a. Review the free credit report for any fraudulent accounts that have been established. Also determine if any unknown inquiries have been made, as these may be indicators of someone attempting to establish a fraudulent account under the customer's name.

5. Contact all financial institutions and creditors where the customer has accounts. The customer should request that they restrict access to the customer's account, change password, or close the account if there is evidence that an account has been the target of identity theft.

First Harrison Bank does not necessarily control the content of the linked sites, nor does it necessarily endorse all of the products and services offered therein.