FIRST NATIONAL BANK OF HUTCHINSON

Equifax Data Breach:
– Frequently Asked Questions and Suggested Action Steps

Q: What happened?

A: Hackers accessed data at Equifax, one of the three major credit reporting agencies.

Q: Who was affected?

A: According to Equifax, 143 million people were affected. About 209,000 people had credit card numbers stolen. About 182,000 people had dispute documents with personal identifying information stolen.

Q: What information was compromised in the breach?

A: Information stolen included records that contained: names, Social Security numbers, dates of birth, addresses, some driver's license numbers, some credit card information, and possibly other information about your credit history.

Equifax indicated that Debit Card information was not exposed.

Q: What if I receive a letter or phone call about Equifax?

A: Scammers will likely try to send emails and make phone calls pretending to help you check the websites, offering credit reporting or other ingenious ways of exploiting the information they know about this breach. Make sure you only go to legitimate sites for anything you do connected to this breach. Do not give out personal information over the phone to anyone who calls you claiming to be an authority on this breach.

Q: What options do I have?

A: If you suspect fraud on any of your accounts or if you'd like to add some additional security, there are several things that you can do. You may:

Enroll in free credit file monitoring and identity theft protection.

Equifax is offering one year of free monitoring, whether or not your information was exposed. Visit https:///www.equifaxsecurity2017.com/ to sign up.

Implement a Credit Freeze or a Fraud Alert on your Equifax and other credit bureau accounts:

Adding a Credit Freeze will help prevent access to your credit information. However, you will need to remove the freeze before you do anything that would require access to your credit report. You will be given a PIN to use to remove the freeze.

Instead of a Credit Freeze you can put a Fraud Alert on your account that lasts 90 days. Whichever bureau you use to add the Fraud Alert (Equifax, Experian, or Trans Union) will report to the other two bureaus as well.

Keep in mind that putting a Credit Freeze or Fraud Alert on your account may make it harder for you to apply for loans, credit cards, or other things for which institutions may check your credit.

Pull Credit Report(s):

You are entitled, by law, to a free credit report from each of the credit bureaus once a year. You can get this at http://www.annualcreditreport.com/ or by calling 1-877-322-8228. Be wary of scams suggesting different links.

Add a password to your banking account(s) and monitor them frequently:

Call The First at 620.663.1521 or 800.310.1521 during banking hours, to put passwords on your account(s). While the Equifax hackers didn't get bank account numbers in this breach, they can see loan history.

Do not wait on paper statements to arrive in the mail. Take advantage of online and mobile banking to keep informed of transactions in and out of your account. If you see something you don't recognize, report it to your bank right away. Consider registering for eStatements for even more security.

Contact your credit card companies:

Determine what extra security measures they offer.

Q: Where can I go for more information?

A: There are several sources available.

For more details, including how to place a Credit Freeze or Fraud Alert, click here for additional information on "What to do Post-Breach" from the Financial Services/Information Sharing and Analysis Center.

The Federal Trade Commission provides more information at: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

You can learn more about how to protect yourself after a breach by visiting: https://www.identitytheft.gov/Info-Lost-or-Stolen