What Happened? The personal data of approximately 143 million US consumers from the credit reporting agency, Equifax, was obtained by hackers through a system breach. Hackers obtained full legal names, social security numbers, birth dates, legal addresses and some driver's license numbers. In addition, the hackers obtained 209,000 credit card numbers for US consumers and the personally identifiable records on approximately 182,000 individuals.This historical breach may be most harmful to consumers that are in the market to purchase a home. To get a sense of how widespread the breach was, consider this simple math; If there are roughly 236 million US adult consumers with credit and 143 million of their credit records were stolen, that amounts to approximately 60% of the US adult population with a credit history. That is a staggering number given the level of information that is now in the hands of cyber criminals.

How will this Affect the Real Estate Industry? This breach will have long lasting impact on the lending, real estate and title industries. The home buying process is highly dependent on the buyer's ability to obtain a loan for the purchase which, in turn, is conditioned upon the credit worthiness of the buyer. The information obtained in the Equifax breach arms cyber criminals with all the information needed to open new lines of credit which could jeopardize someone's ability to qualify and/or close on a mortgage loan. More concerning is that certain types of payday loans or other non-traditional loans may not be reported to the credit bureau so they could be opened and go into default without any way of knowing.

Was Your Information Breached? Equifax has a website to confirm whether your information has been breached. The website is: www.equifaxsecurity2017.com/potential-impact .   The site will ask for some personal information and will confirm you are not a robot. It will immediately let you know if your information was compromised. Here's a screenshot of what will be displayed:

Thank You

Based on the information provided, we believe that your personal information may have been impacted by this incident.

Click the button below to continue your enrollment in TrustedID Premier.

Enroll

For more information visit the FAQ page.

My Information Was Breached – What Now? There are several things that should be done to protect you from fraud relating to this breach. While not an exhaustive list, here are some simple things you could payoff in the long run:

1. Enroll in Equifax's Identity Protection Program. Equifax is offering to enroll anyone in its identity protection program, Trusted ID. The program acts as a solution to prevent identity theft and credit tampering. To register with Trusted ID, go to: https://trustedidpremier.com/consumer-registration/html/personal-info.html. You will be asked to include your personal information and once submitted, you will receive the following notification:

Thank You

We have successfully received and are processing your information.

Next Step

You will receive an email with a link to finalize your enrollment and activate your product. Please be patient. Due to the high volume of requests, emails may be delayed. If you have not received your email within a few days, please check your spam and junk folders.

Thank you again; we appreciate your patience!

2. Institute a "Freeze" on Your Credit. You can request a credit "freeze" which is a tool that restricts access to your credit report. This should make it more difficult for cyber criminals to open accounts in your name. There is a fee of around $10 per bureau to initiate a "freeze" and a similar fee to lift the freeze. Once you initiate a freeze, you will be mailed a secure code that you will need to provide to lift the freeze. For more information on the credit freeze, visit the Federal Trade Commission website at: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs. To initiate a credit freeze you need to contact each of the three credit bureaus directly through the following:

    Equifax: 1-800-349-9960 or https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
    Experian: 1-888-397-3742 or https://www.experian.com/freeze/center.html
    TransUnion: 1-888-909-8872 or https://www.transunion.com/credit-freeze/place-credit-freeze

3. Monitor Your Credit Report. The US government allows everyone a free credit report each year from the three credit bureaus. You need to set reminders to pull and review these reports at least twice per year. If you are obtaining financing for a transaction, make sure you receive a full credit report from the financing institution and review it closely for anomalies add odd lines of credit that are unfamiliar. For information on the free credit report program and how to obtain a copy visit: https://www.consumer.ftc.gov/articles/0155-free-credit-reports. You may also monitor your credit through services like Credit Karma (www.creditkarma.com).

4. Initiate a Fraud Alert. You can set an alert that will notify you if cyber criminals attempt to open accounts using your stolen information. This is a third layer of protection that is easy to add. For information on the placing a fraud alert on your credit profile simply visit: https://www.consumer.ftc.gov/articles/0275-place-fraud-alert

5. Review Credit Card and Bank Statements.   The personal information stolen from Equifax took place over the past three months. It is important to take a close look at all credit card and bank account transaction statements. Cyber crime often starts out small as the test the waters and then they strike hard once they feel that no one is watching. Diligence in this area will payoff in the long run.