

September 2017

It has been widely reported that Equifax, one of the three main credit reporting companies, suffered a major data breach that exposed Social Security numbers and other vital information of millions of people.

About 143 million people in the United States were affected by this breach. Data was available to hackers in May and July. The hackers had access to Social Security numbers, dates of birth, addresses, credit card numbers and other information.

Before we share some steps to help protect your credit, we want to go over exactly what is included on your credit report:

Personal Information

Name, address, Social Security number, date of birth and employment information. This information is not used to score your credit.

Trade Lines

Credit accounts. Lenders report on each account you have established with them. This includes the type of account (credit card, mortgage, auto loan, etc.), date accounts were opened, credit limit, account balance and payment history.

Inquires

Inquiries occur when a lender asks for a copy of your credit report. The inquiries section is a list of everyone that has accessed your report within the last two years.

Public Records and Collections

Public record information from state and county courts. Overdue debt from collection agencies, bankruptcies, foreclosures, suits, wage garnishments, and liens are also included.

What is not on your credit report

A few things not included in your credit report are your bank account number(s) and balances and investment account number(s) and balances.

So, what action can you take?

There are a number of steps that you can take to protect your credit and identification. The first, confirm if you have been impacted by this incident. You can do this by visiting <https://www.equifaxsecurity2017.com/potential-impact/> and entering your last name and the last 6 digits of your Social Security number. Additionally, Equifax has setup a dedicated call center to answer basic questions regarding the breach. You can contact them directly at 866-447-7559. Be prepared for long wait times.

If you have been impacted, it may be wise to take one or more of the following steps to protect yourself.

Do a Credit Check

Consider checking your credit with the three credit agencies, Equifax, Experian, TransUnion. This can be done for free by visiting <https://www.annualcreditreport.com/>. If you see suspicious activity on your report contact the affected entity and the reporting agency.

Freeze Your Credit

A credit freeze will make it more difficult for someone to open a new account in your name. It cannot, however, stop a thief from using one of your current accounts. To apply for new credit, you will need to unfreeze your credit.

Monitor

At a minimum, closely monitor your credit card and bank account activity. Most banks and credit cards offer alert services which can be configured to send you an email when there is activity on your accounts. Contact your bank or credit card company immediately if you see suspicious activity.

ID Theft Protection

Sign up for an ID theft protection plan through companies like LifeLock, Experian, and IdentityForce. These services provide the monitoring and protection on your behalf. Fees for this range from \$10 to \$30 per month.

Take caution with phone calls or emails that claim to be from the credit agencies especially Equifax. If you have any questions please feel free to call our office at 503-905-3100 to speak with either Jill Novak or myself, Kevin Wilson.