WILLMS, S.C.

MEMORANDUM

TO: Clients and Friends of Willms, S.C.

DATE: September 13, 2017

SUBJECT: Equifax Data Breach

As you may know, on Thursday, September 7th Equifax, a large consumer credit reporting agency, announced that it was the target of a cyber-attack. The hack resulted in the personal identity information of nearly 143 million people being compromised. The following summarizes what you should know about the cyber-attack, provides information on how to find out if your personal information may have been compromised, and describes actions that you can take in an effort to protect your data.

Things you should know:

1. Equifax collects personal information from credit card companies, banks, mortgage lenders, etc. and provides that information to lenders, banks and the like when you open credit cards, apply for loans, etc. As a result, your personal information could have been compromised even though you are not an Equifax customer.

2. Equifax cannot definitively tell you if your personal information is compromised. However, Equifax has provided a security site where you can check if your information ***may*** have been compromised.

How to check if you have been potentially affected:

Equifax has established a website where you can check if your personal information may have been compromised. To do so you must enter your last name and last six digits of your social security. The site will then notify you if your personal information "may" or "believe not to" be compromised. The following link will take you to the website:

https://www.equifaxsecurity2017.com/potential-impact/

You can also monitor's Equifax's progress on dealing with the cyber-attack here:

https://www.equifaxsecurity2017.com/

What cyber security experts are recommending you should do if your personal information may have been compromised:

1. Check your credit report**.** You can obtain a free credit report here:

   https://www.annualcreditreport.com/index.action

   This will allow you to identify any suspicious activity that may have occurred due to this cyber-attack or any other fraudulent activity. We also recommend you mark your calendar to periodically check your credit report to identify any potential future fraudulent activity. We also suggest you get your annual Social Security benefits statement online here and check for anything unusual.

   https://secure.ssa.gov/RIL/SiView.do

2. Be on guard. Watch out for unusual mail and be careful when responding to suspicious email. Check your bank accounts frequently for signs of fraud.

3. Get Identity Theft Protection**.** Equifax is currently offering free identity theft protection, but some commentators are questioning the appropriateness of the terms and conditions of the offer.

4. Set up fraud alerts**.** This will enable you to receive alerts if any perceived fraudulent activity is being used with your personal information. You can set up these alerts with any of the major credit reporting agencies, such as TransUnion, Experian, and Equifax.

5. Consider Putting a Freeze On Your Credit Report. A credit freeze provides valuable protection because it will prevent companies you already do business with (i.e. banks, credit card companies, mortgage lenders, etc.), from providing your credit information to other parties without your consent. However, a credit freeze could also restrict your ability to open new credit cards, obtain loans, etc. so you should carefully consider whether a credit freeze is appropriate in your situation. You can learn more about the pros and cons of a credit freeze, and how to obtain one, here.

   https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

We hope you find the foregoing information of assistance. Please let us know if we can be of further assistance. Thank you.

End of Memo