The Equifax Breach and You

On September 7, 2017, credit-reporting agency Equifax announced that it experienced a data breach earlier in the summer. The attack impacted the sensitive and personal information of around 143 million people. The attack occurred due to software vulnerability in a web application framework that Equifax used – Apache Struts. Although Apache had released a patch, or update, to fix the vulnerability, Equifax apparently had not implemented the fix at the time the breach occurred.

What Are the Authorities Doing About This?
Equifax and the incident are the subjects of investigations by at least one congressional committee, the Federal Bureau of Investigations (FBI) and the Federal Trade Commission (FTC), as well as nearly 40 state attorneys-general. Legislation to tighten security requirements for databases compiling personal information has also already been introduced in Congress.

Direct Claims Against Equifax in the Courts
There have already been upwards of twenty lawsuits filed against Equifax by consumers claiming harm from the data breach. At least one state, Massachusetts, has also brought suit on behalf of its citizens.

As the Consumer, What Should You Do?

1. *Determine if the Breach Exposed Your Information.* Equifax has created a unique website dedicated solely to breach matters – https://www.equifaxsecurity2017.com. Within that website, you can check your "potential impact" — that is, whether Equifax believes your data is at risk. Whether or not evidence indicates that intruders accessed your personal information, Equifax is offering its TrustedID Premier credit monitoring and identity theft deterrent services to the public free for one year.

Taking advantage of the monitoring service, while likely helpful, may not be sufficient to completely address the risk of identity theft and misuse of your personal information. If your Social Security number, driver's license, birth date, and other such fixed, permanent information falls into the wrong hands, misuse could occur years or even decades later. Maintaining security for your personal information is a lifelong exercise.

2. *Consider a "Credit Freeze."* In some cases, an individual who is particularly vulnerable to the effects of identity theft may wish to consider a "credit freeze," which is a limitation on the ability of others to review or seek to modify your financial or credit-related personal information. However, this method may also be burdensome or unworkable for a person who is seeking employment, contemplating purchase of a house, or anticipating a significant financial transaction.

3. *Change Your Passwords – Regularly.* Regularly changing your passwords is good practice in the best of circumstances. Changing passwords becomes critical when there is an increased risk that your sensitive personal information may be circulating among hackers. Armed with your sensitive information, a hacker may be able to contact banks and companies you do business with, impersonate you, and convince a bank or other company to change your account information.

4. *At Least Once a Year, Obtain and Review Your Credit Information.* Unauthorized credit inquiries and extensions of credit are frequently the first indication that online criminals are using your personal information. A good way to spot such activities is to actively monitor

your credit information. The FTC has recommended instructions on how to get your credit report.

What Should Your Company do if a Breach Occurs?
Equifax is a large corporation and its compilation of sensitive financial and credit information is a particularly attractive target for hackers; nevertheless, billions of intrusion attempts are made each year on computers connected to the Internet, and any company could be vulnerable. Company management, human resources, information technology, and sales professionals all have important responsibilities to protect company and customer information. Utilizing proper software, protocols, expertise, and maintenance plans go a long way. As significant as the financial consequences of a large breach may be, they are often overshadowed by the damage to a company's reputation and the loss of its customer's trust.

If and when your company does become the target of a data breach, a prompt initial response is critical. Thinking ahead and developing a response plan in preparation for the likelihood of an attempted or even a successful data breach incident may avoid or reduce resulting damages.

After discovering and containing the breach, consider the following:

- Giving adequate and early notice to affected customers and persons whose data may have been compromised is required by almost all states and under some circumstances by federal law.

- Time limits in some states for very sensitive information can be as short as five days after discovery of the breach.

- The form and content of the notice is also prescribed in a number of states.

- Transparency is vital – transparency with the company's employees, its consumers, and its stakeholders. Ideally, interested parties should hear about the breach from you – not in the news.

Need Help?
If you think you have been affected by the Equifax breach – or any other data breach – and want to discuss the legal issues involved, feel free to contact us. If your company is ready to take a closer look at your data protection policies or create a cyber incident response plan, we'd like to help.

RELATED ATTORNEYS:
James K. O'Brien
Silvia A. Mansoor