WALKER WILCOX
WALKER WILCOX MATOUSEK LLP

EQUIFAX BREACH: SUMMARY, STATUS AND SIGNIFICANCE

What Happened: On September 17, 2017, Equifax, one of the "big three" credit bureaus, announced that a data breach exposed confidential information for about 143 million individuals in the U.S., Canada and the U.K. Equifax discovered the breach weeks earlier on July 29, 2017. The data disclosed includes names, addresses, dates of birth, social security numbers, credit card and driver license numbers. Equifax claims the intruders exploited a vulnerability in its software program called Apache Struts starting in May 2017.

Within days of the announcement, Equifax was named in dozens of class actions and in investigations by the FTC, CFPB, Department of Justice, state and municipal governments. Equifax's stock dropped 35% within a week of the announcement. Equifax fired its CEO, CISO and CSO. Two congressional hearings will seek testimony by Equifax executives.

Is the Equifax Breach Different? Many consumers and businesses are numb to massive data breaches. It seems that "the largest breach ever" occurs regularly. So is the Equifax different from other massive breaches? In several respects, yes. What pushes Equifax to a new level is the combination of the breach size and the type of data involved. Almost every adult in the country with a credit history is affected. A name, DOB and social security number are considered the "trinity" of personal identifiers. In particular, a stolen social security number may have life-long consequences. It cannot be changed like a credit card and can be used to open a bank account, take out loans, obtain health care and file fraudulent tax returns.

Unlike retailers, Equifax does not have "customers" whose loyalty is at risk. The consumer cannot control which credit bureau a bank or landlord uses to check credit history. Equifax's business is collecting consumer data, and anyone with a credit history eventually becomes the Equifax product. Some critics say this explains Equifax's indifference to the breach – reporting delays, requiring consent to arbitration before confirming a consumer's involvement, charging for credit freezes and repeatedly posting a bad link for consumers on its social media account.

Another significant aspect of the Equifax breach is the aggregation of losses across cyber and non-cyber policies. The publicity has focused on the risks to consumers. But what has received less attention is the number of business products that Equifax provides. Equifax offers data products to 12 industries, ranging from automotive to staffing. For example, many employers use the Equifax wage and employment verification system. Equifax provides a bankruptcy alert that informs a business client if a commercial business has filed for bankruptcy. Equifax uses consumer data to marketing targets for insurers, retailers, restaurants, credit unions and small banks. Governments rely on Equifax's data for security clearances. All these businesses may incur costs to verify the integrity of Equifax's data. Companies that provided consumer data to Equifax may be accused of negligently entrusting sensitive data to a company with deficient risk management practices.

WALKER WILCOX

WALKER WILCOX MATOUSEK LLP

Click here for PDF.