# Equifax Breach a Category 4 or 5 Attack, but By No Means Unique

**Late last week, we learned that Equifax was breached via a simple web application weakness, and over 143 million consumers' records were compromised. These records weren't salacious emails or leaked Game of Thrones episodes; these were the Social Security numbers, home addresses, and the most sensitive financial data of millions of Americans.**

As U.S. Senator Mark Warner, a founder of the bipartisan Senate Cybersecurity Caucus, stated, this breach was "a category 4 or 5 cyber hack," representing "a real threat to the economic security of Americans."(1) The bad (worse) news is that this story is not unique, and this is by no means the final chapter.

## Why Equifax?

Why was Equifax targeted? Well, consumer credit reporting agencies are warehouses for sensitive personal data, which makes them attractive targets for hacking. The information that Equifax stores is highly desirable for criminals to perpetrate phishing scams, tax return fraud, identity theft and more. The richness of this private data definitely played a role in why the company was targeted. We certainly can expect to see more corporations and law firms that deal in sensitive data finding themselves in the crosshairs of hackers.

## The Implications

No doubt about it, this is a massive and serious data breach that will likely affect every family in America; however, this is not the first serious hack to a major company or organization that has compromised the data of millions of Americans, nor will it be the last. The Equifax breach is just the latest in an emerging trend of cyber hacks and sabotage across all industries, and it underscores the need for adopting strong cyber threat prevention measures. As a custodian of sensitive data that was not directly supplied to them by consumers, Equifax bore a burden, perhaps heavier than that of others, to protect that data.

## The Consequences?

There is a huge fallout when things like this happen. In just one day Equifax's stock fell some 14%. There has been criticism from regulators and influential cybersecurity lawmakers such as Senator Warner; a federal investigation has been opened by the Attorney General of New York; and a class-action lawsuit that promises to be massive has already been filed. Further, this incident may irreparably degrade the public's confidence in the security of their personal information when it resides with corporations.

## What's Next?

There are a number of financial, operational, reputational, and legal implications when data breaches occur, and companies should be forward-thinking in how they seek to prevent and mitigate potential cyberattacks. It's critical that companies invest in securing their systems and assets to not only prevent threats like these, but to preserve consumer confidence and the integrity of their business and brand.

(1) U.S. Senator Mark Warner, *CNBC*, 9/8/2017, http://www.cnbc.com/video/2017/09/08/sen-mark-warner-equifaxs-breach-is-a-category-4-or-5-cyber-hack.html

**Anthony J. Ferrante**
Head of Cybersecurity & Senior Managing Director
FTI Consulting, Inc.
202.312.9165
ajf@fticonsulting.com

FTI CONSULTING | CYBERSECURITY