THOUGHT FOR THE WEEK
WHAT CAN INVESTORS LEARN FROM THE EQUIFAX HACK?

Global Financial Private Capital

SYNOPSIS

- Equifax has dominated headlines recently due to a security breach that may have compromised personal information for as many as 143 million Americans.
- Equifax is in the business of storing highly-sensitive data, so it's not surprising that hackers targeted them.
- Markets evolve over time, and one of the easiest ways to lose money is to refuse to adapt to them.

EQUIFAX HACKED

Equifax has dominated headlines recently due to a security breach that may have compromised personal information for as many as 143 million Americans. According to the United States Census Bureau, approximately 323 million people lived in the U.S. in 2016. Therefore, roughly 44% of Americans are at risk from this intrusion.

Identity theft is nothing short of a nightmare for its victims, so investors are understandably anxious to protect themselves. An effective tactic to guard against theft is to freeze your credit with each of the major credit bureaus.

Imagine a situation where a thief stole personal information and then used it to apply for a credit card. The first step in the bank's approval process would be to conduct a routine credit check to verify the applicant's information and analyze their credit history.

If the victim had a "credit freeze" on the account, the credit bureau would deny any request to access the file. The bank would not be able to complete the credit check, which would most likely deny the credit card application submitted by the criminal.

There are four main credit bureaus, so anyone interested in freezing their credit must contact each agency. Some states also allow credit bureaus to charge a small fee, so be prepared to pay (Equifax has stated that they will not charge for this service).

The process is pretty straightforward. Once you provide your information, each agency will issue a Personal Identification Number (PIN) that can be used to unfreeze your file in the future. The table below lists the web addresses to begin the process at each of the major credit bureaus.

Equifax	www.freeze.equifax.com
Experian	www.experian.com/freeze/center.html
TransUnion	www.transunion.com/credit-freeze/place-credit-freeze
Innovis	innovis.com/securityFreeze/

WHAT'S NEXT

Equifax is in the business of storing highly-sensitive data, so it's not surprising that hackers targeted them. Most large financial and data-driven companies are under constant attack and spend millions each year in defense systems to thwart these criminals.

However, what is truly mind-boggling is how easily the hackers got in and the questionable judgement displayed by senior leadership once they discovered they had been hacked.

"...the last thing an investor or a consumer should ever do is throw the baby out with the bathwater."

The short version of the story is that Equifax's security team was notified earlier this year that a vulnerability existed in their network and was instructed to install a software patch. For whatever reason, they did not upgrade their systems, which kept the door open for hackers to walk right in and take a bunch of data.

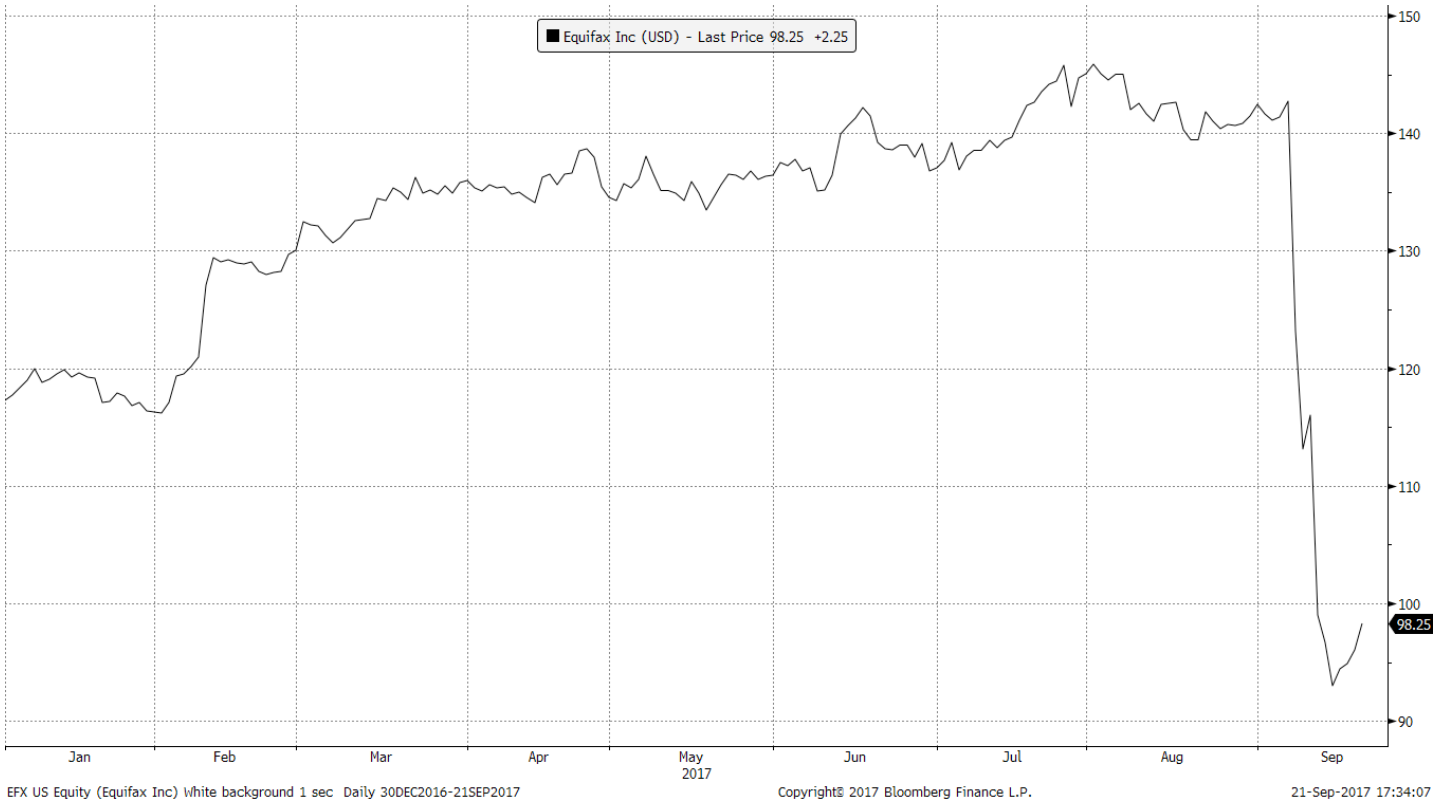
The intrusion went undetected for over a month, and rather than warn consumers the instant they discovered they had been hacked, management spent several more

WHAT CAN INVESTORS LEARN FROM THE EQUIFAX HACK?

weeks conducting an internal investigation to estimate the extent of the damage (giving the criminals even more time to do bad things with the stolen data).

Making matters worse, three Equifax senior executives, including the Chief Financial Officer, sold shares worth almost $1.8 million in the days after the company discovered the breach but before they disclosed it to the public[1].

The chart below shows the reaction of company's stock to the news, and the stock sale begs the question of whether these executives were aware of the intrusion when they submitted their trade requests.



Source: Bloombeg

The timing of these transactions will most certainly be investigated, and even if the authorities determine that this was nothing more than a coincidence, the court of public opinion will likely return a different verdict.

With respect to the future for Equifax, it's too early to tell if the firm will survive this debacle, but it's safe to say that heads will roll. The Chief Security Officer, who interestingly earned both a bachelor's degree and master of fine arts in music composition but has no mention of technology or security on her LinkedIn profile[2], has "retired."

The Chief Information Officer has also chosen to leave the firm. I would not be surprised to see the Chief Executive Officer ousted in the coming months. The board of directors will likely want to clean house as a first step to rebuilding confidence in their customer base.

Where I am more certain is in the future for the credit bureaus because the media attention and consumer outrage will demand a swift response from politicians. These firms should expect to see a material increase in government oversight and regulation in everything from how they store data to education and experience requirements for key personnel. Simply put, their cost of doing business will most likely rise.

IMPLICATIONS FOR INVESTORS

Rewind the clock not that long ago and cyber-attacks rarely made headlines because their impact was limited. However, as the digital age continues to evolve, these risks are becoming more complex with the ability to cause even greater damage.

Hackers today are well-educated and well-funded (many are sponsored by governments with very deep pockets), and the need to fight them will drive further innovation in cybersecurity. Corporate boardrooms can no longer ignore these threats as accountability continues to fall more on their shoulders.

These risks will also require a change in consumer behavior, and it's important to move forward rather than backward to shield ourselves from the risks associated with technological progress.

For example, a natural reaction to the fear of identity theft is to withdraw all assets from the banking system and stuff the cash under a mattress. This strategy would certainly prevent a hacker from stealing a nest egg, but in reality, it is moving backward.

Storing physical cash would do little more than swap the risk of virtual theft with substantially larger risks like physical theft and damage. Cash in the banking system is protected within a highly-regulated industry and usually insured up to $250,000.

Stuffing cash under a mattress puts the onus of protection on the individual rather than the banking system. Said another way, where there is recourse for those who have been hacked, there is not much one can do if their cash is stolen in a burglary or incinerates in a fire.

The same lessons can be applied to investing. Financial markets also evolve over time, and new risks develop alongside this progression. Investors can lose money when they refuse to recognize these risks or address them by taking steps backward rather than forward.

A current example is the two options facing investors when responding to rising interest rates.

The first is to sell all bonds and go to cash. However, much like emptying a bank account and stuffing bills under a mattress, this is taking a step backward by swapping one risk for a far more dangerous one.

Bonds aim to provide diversification[3] in addition to steady income, and they are an important component to most asset allocations. Furthermore, the return on cash investments will most likely fail to exceed inflation for years to come, so all this option does is ensure that an investor loses money "safely."

The second is to change how an investor is positioned in the bond market. Use a new playbook that is specifically designed for rising interest rates by fishing in different ponds and searching for opportunity that flies under the radar of other investors.

This option will likely to be the road less traveled for two reasons. First, it's human nature to fear what we do not understand, and second, it will require more work and/or the assistance from highly-skilled navigators. But this is the option investors should consider because it focuses on where markets are going rather than where they have been.

In the end, it all comes down to recognizing that technological progress will continue whether we like it or not. New risks will spawn from this advancement, but that is the byproduct of innovation. The good news is that despite the risks, society tends to benefit far more than hurt from these productivity gains.

The same applies to financial markets. Just because new risks develop over time does not imply that the world is going to end. It is simply a byproduct of this evolution and evidence that achieving financial goals will most likely require moving an investment strategy forward.

WHAT CAN INVESTORS LEARN FROM THE EQUIFAX HACK?

The bottom line is that when addressing risks associated with change, the last thing an investor or a consumer should ever do is throw the baby out with the bathwater.

Sincerely,

Mike Sorrentino, CFA

Chief Investment Officer,
Global Financial Private Capital

[1]*https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack*

[2]*https://www.linkedin.com/in/susan-m-93069a/*

[3]*Diversifcation does not ensure a profit or guarantee against loss*