USA Today

SEC hack unsettling for 401(k) and pension savers, but it's no Equifax

By Adam Shell
Sept 21, 2017

The Securities and Exchange Commission was in the hot seat after it admitted hackers made their way into its EDGAR electronic filing system last year and made off with information it believes might have been used to make money illegally in the stock market.

U.S. lawmakers were stung by the news, late Wednesday, of the breach of the SEC's sensitive corporate data -- a disclosure that comes just two weeks after Equifax, one of the nation's three largest credit bureaus, revealed that hackers were able to access the private financial data of 143 million people.

A Senate banking committee will seek answers Tuesday in Washington, when members, at a previously scheduled hearing, will likely grill SEC chairman Jay Clayton -- who took over the SEC's top post in May -- on the timeline and details of the data breach.

The breach involving Wall Street's top cop may be unsettling "burglary" of market-moving data, but it's no Equifax in terms of consumer exposure. However, the hack that allowed cyber thieves to burrow into a government regulator's database filled with millions of corporate filings about earnings, mergers and digital trading footprints does little to instill confidence in the integrity of the market that millions of Americans depend on to fuel their 401(k) and pension investments.

"It won't make mom-and-pop investors feel comforted to know that the regulator keeping their investments safe got hacked," says **Joe Saluzzi**, co-founder of **Themis Trading** and co-author *Broken Markets*.

Members of the House of Representatives also say they are in fact-finding mode. In an interview with USA TODAY, Congressman Bill Huizenga of Michigan, chair of the House subcommittee on Capital Markets, Securities, and Investment, said: "We all need to dive in more deeply as to what happened here."

What troubles Huizenga is the fact that everyone knows the SEC is a prime target of hackers, "and clearly not enough attention was paid to securing" the corporate data in its filing system.

"We can't view this as a victimless crime. It was a burglary. Market-moving information like that has got to be protected," said Huizenga. "Regulators have to be held to the same standard as the companies and (market players) they are regulating."

But security experts say the financial fallout for everyday Americans might not be as bad as feared.

"This hack is different than the Equifax or Target hacks," says Lev Lesohkin, executive vice president of New York-based CAST, a software intelligence company. "The hackers (in the SEC data theft) are not going after consumer data" that could be used to steal a person's identity

It was only in August that the SEC learned that hackers may have been able to use their illegal activities to make ill-gotten gains through market trading, said SEC's Clayton in astatement posted on the SEC's website late Wednesday.

EDGAR, which stands for Electronic Data Gathering Analysis and Retrieval, is considered critical to the SEC's operation and the ability of investors to see the electronic filings of companies, brokerage firms

and mutual funds. The SEC says about 50 million documents are viewed through EDGAR on a typical day. It receives about 1.7 million filings a year.

While most filings are made public immediately, ones that require SEC feedback at times, such as quarterly and annual reports or documents related to companies about to sell stock to the public for the first time, are not. It is these types of non-public data that can be stolen and traded upon illegally by hackers, analysts say.

Lesohkin's theory is the SEC attack was executed by sophisticated hackers that understood how they could profit by extracting market-moving data from the EDGAR system.

For example, hackers might have targeted what the SEC calls its Consolidated Audit Trail, or CAT.

CAT provides what amounts to a digital trading footprint, that facilitates "the efficient tracking of trading activity" in the stock market, the SEC's Clayton noted in his statement.

For example, if a hacker found out in a filing that, say, Warren Buffett was building a huge stake in a stock unbeknownst to the marketplace, a hacker could profit on that information by buying the stock before the rest of the market found out and it rose in price, says **Saluzzi**.

This is not the first time the SEC's EDGAR system has been infiltrated by cyber thieves. In May, the SEC filed fraud charges against a man that schemed to manipulate the price of Fitbit stock by "making a phony regulatory filing." Similarly, on May 15, 2015, a fake financial firm put in a fake filing with the SEC claiming it was buying cosmetics company Avon for $18.75 a share, at the time the stock was trading at $6. Avon shares shot up, and trading in the stock was halted three times that day before the fraud was determined.