The New York Times | https://nyti.ms/2wPtl6g

BUSINESS DAY

Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable

By TARA SIEGEL BERNARD and STACY COWLEY SEPT. 8, 2017

Equifax warehouses the most intimate details of Americans' financial lives, from the credit cards in their wallets to the size of their medical bills.

But the company doesn't face the constant monitoring and auditing that help strengthen banks' systems and data protections. Despite the wealth of sensitive information in its databases, Equifax, in essence, falls through the regulatory cracks.

The dangers of such lax oversight became apparent on Thursday when Equifax disclosed that hackers had compromised the personal and confidential information, including Social Security numbers, of nearly half of the American population.

Equifax is now scrambling to contain the legal and financial fallout.

New York's attorney general, Eric T. Schneiderman, has opened an investigation into the data breach, while two potential class-action suits have been filed. Shares of the company were down nearly 14 percent on Friday.

A consumer backlash is growing over the company's response to the breach. The remedy that Equifax has offered — one year of free credit monitoring — struck many as inadequate. Compounding the frustration, three senior executives, including the chief financial officer, sold $1.8 million worth of shares in the days after Equifax discovered the breach.

Equifax and two other consumer credit bureaus, Experian and TransUnion, create the reports used to calculate credit scores, the ubiquitous three-digit numbers that banks, insurers, lenders and employers rely on to make all manner of decisions. Those scores, the algorithmic assessment of a consumer's entire financial history, help decide whether somebody gets a job or a new home.

The bureaus each have files on roughly 200 million Americans. And consumers have little choice, since banks and other companies hand over financial information and other data directly to the bureaus. The industry has been marred by complaints of mistakes on credits reports and difficulties in fixing them.

The data breach at Equifax, which affected 143 million people, could compound the problems, leaving consumers vulnerable to identify theft. It was the third hacking disclosed by Equifax this year.

“You cannot fire the three credit bureaus,” said Rohit Chopra, a former assistant director at the Consumer Financial Protection Bureau and now a senior fellow at the Consumer Federation of America. “Credit reporting agencies are the plumbing of our financial system but are much less regulated than many banks.”

TransUnion said it was investigating the nature of Equifax’s attack and what, if any, actions might be appropriate. Experian and Equifax did not return calls for comment. Equifax released a statement apologizing to customers for “the concern and frustration this causes.”

The credit bureaus fall into something of a regulatory gray area in Washington.

They are covered by many of the same data security laws that apply to banks. But banks face much stricter oversight, with a team of agencies working together to audit institutions and monitor their compliance. Non-bank companies, like the credit bureaus, generally are scrutinized only after something has gone wrong.

Federal laws require all companies to take reasonable steps to safeguard consumer data. While the Consumer Financial Protection Bureau has some supervisory and enforcement authority over the credit bureaus, the agency generally leaves data privacy enforcement to the main regulator in charge of it, the Federal Trade Commission. And the trade commission lacks the authority to impose big fines.

Last month, the commission punished TaxSlayer, a tax preparation website, for a weak security system that allowed hackers to gain access to nearly 9,000 customer accounts. TaxSlayer agreed to strengthen its systems and undergo compliance audits. But it paid no financial penalty, because the commission has no power to levy fines for first-time violations of certain rules.

“Both in terms of resources and authority, what the F.T.C. can do clearly doesn’t measure up to the scale of the problem,” said William McGeveran, a professor at the University of Minnesota Law School who specializes in privacy law.

A spokeswoman for the Federal Trade Commission, Juliana Gruenwald Henderson, said the agency does not comment on its investigations and declined to say if it had opened one on Equifax.

The Consumer Financial Protection Bureau is "looking into" the data breach at Equifax, according to Sam Gilford, a spokesman, but he declined to comment further.

Credit reporting is big business. Equifax made $3.1 billion in revenue last year, collecting the vast majority from businesses like banks and other financial service companies.

But the industry has been the subject of criticism over its data collection and reports. In some examples, two people were combined into a single file. In other instances, the bureaus have inserted a person's information into the wrong credit report, which can occur when two people have similar Social Security numbers.

Two years ago, a coalition of more than 30 state attorneys general cracked down on the credit bureaus, negotiating a deal that required sweeping changes. The bureaus dropped some error-ridden data sources from their reports and agreed to provide more information to consumers who disputed data on the reports.

Problems have persisted. This year, Equifax and TransUnion agreed to pay a combined $23 million to settle allegations by the

Consumer Financial Protection Bureau that they made “false promises” to lure customers into buying credit-related products. Those products were promoted as free, but came with monthly fees if customers didn’t cancel during the trial period.

The data breach at Equifax could expose the company to legal and financial challenges, although the regulatory environment isn’t likely to become stricter under the current presidential administration.

On Friday, Representative Ted Lieu, Democrat of California, sent a letter to the leaders of the House Judiciary Committee calling for a hearing to address the breach. In his letter, Mr. Lieu asked that representatives of the three bureaus be called to testify about what steps were being taken to prevent future intrusions.

“Congress has a strong role to play in preventing such attacks on our financial and I.T. infrastructure, and must hold those entrusted with our most sensitive data to account,” Mr. Lieu wrote in the letter.

As consumers digested the scope of the hacking, a website set up by Equifax to help was inundated. The site purported to determine whether people’s data was compromised, after visitors entered six digits of a Social Security number and other information.

It offered only vague responses, saying personal information was not impacted or that it "may have been impacted." People who used the site quickly noticed that entering bogus names and numbers often generated the same messages.

"It requires trust where there is no trust," said Justin Baxter, a consumer lawyer in Portland, Ore., who is an attorney in a suit seeking class-action status against Equifax. "Asking people to type in personal information to find out if their personal information has been breached — a lot of people are not going to do that."

Equifax also recommended signing up for a monitoring services. But the program initially required users to give away their rights to legal action and agree to use arbitration to settle disputes.

It immediately drew outrage, with Mr. Schneiderman, the New York attorney general, calling on Equifax to remove language that could deny victims the right to sue. Equifax has since changed the clause, giving consumers the ability to opt out.

The company is now offering one year of free credit monitoring to all consumers, not just victims of the breach. It is also providing people the ability to freeze their Equifax reports, which, in theory, should prevent thieves from applying for credit in their name.

"This is a one-year solution for an eternal problem," said Adam Levin, chairman of CyberScout, which provides data breach defense services. "The collateral damage can be devastating, and when you are talking about Social Security numbers the only expiration date a Social Security number has is yours."

Tiffany Hsu, Susan C. Beachy and Matthew Goldstein contributed reporting.

A version of this article appears in print on September 9, 2017, on Page A1 of the New York edition with the headline: Equifax Is Facing Harsh Scrutiny. If Only It Had Come a Bit Sooner.
