The New York Times https://nyti.ms/2jSPZb2

BUSINESS DAY

As Equifax Amassed Ever More Data, Safety Was a Sales Pitch

By STACY COWLEY and TARA SIEGEL BERNARD SEPT. 23, 2017

Equifax's chief executive had a simple strategy when he joined more than a decade ago: Gather as much personal data as possible and find new ways to sell it.

The company was making good money compiling credit reports on Americans. But Wall Street wanted stronger growth.

The chief executive, Richard F. Smith, delivered, releasing dozens of new products each year and doubling revenue. The company built algorithms and started scrubbing social media to assess consumers. In a big data collection coup, Equifax persuaded more than 7,000 employers to hand over salary details for an income verification system that now encompasses nearly half of American workers.

As part of its pitch to clients, the company promised to safeguard information. It even sold products to help companies hit by cyberattacks protect their customers.

"Data breaches are on the rise. Be prepared," the company said in one pitch. "You'll feel safer with Equifax."

But this strategy means that Equifax is entrenched in consumers' financial lives whether they like it or not — or even know it. Equifax's approach amplified the consequences of the breach, reported this month, that exposed the personal information for up to 143 million people.

Ordinary people are not Equifax's customers. They are the company's product. The "Big Three" credit bureaus, Equifax, Experian and TransUnion, collect 4.5 billion pieces of data each month to feed into their credit reports.

From birth to death, the record grows. Decades' worth of addresses and identifying information, including drivers' licenses and Social Security numbers. Utility accounts like telephone and cable subscriptions. Criminal records, medical debt, as well as rental and eviction histories.

Equifax's records on any given individual, scattered throughout dozens of databases, typically stretch across hundreds or thousands of pages.

Equifax now faces a consumer backlash over its response to the hacking attack. The anger has been intensified by the actions of three senior executives who sold shares worth $1.8 million in the days after the breach was discovered. The stock, which had tripled in the last five years, is down 30 percent since the attack. Equifax said the executives were unaware of the breach when they sold their stock.

Customers have been less vocal, given their dependency on the bureaus. Financial firms readily hand over their data because they rely on the credit reports — and the scores they are used to generate — to size up potential customers. The data, over which Equifax and the other bureaus have a stranglehold, is one of the best predictors of risk.

"We don't really have a choice to opt out of the credit report system," said Pete Mills, senior vice president of residential policy at the Mortgage Bankers Association, which represents some of Equifax's biggest clients, home loan providers. "We spend a lot of money trying to protect our customers, and then we give that data to others," like the credit bureaus.

Equifax said it was supporting customers who may have been affected by the data breach. "We value our customers and have been in close communication with them," said Wyatt Jefferies, a company spokesman.

Under Mr. Smith, Equifax has been creative in developing new markets and services. The company expanded globally, often by acquiring local competitors; it now operates in 24 countries.

New analytic products have been a priority. Equifax has a team of mathematicians who mine its data to develop algorithms predicting how consumers will behave. Those insights are sold to companies like lenders.

At a financial conference last year, Mr. Smith described a new system that searched four billion public tweets for keywords like "car" and "automotive lease." It paired the tweets with a person's Equifax credit file. In real time, the credit bureau could identify potential buyers and provide its customer, a company selling car leases, with everything it wanted to know about those people.

The corporate culture shifted under Mr. Smith and became more focused on increasing profit, said David Galas, who left Equifax in 2011 after 13 years.

"It was run a little more like a sports team," said Mr. Galas, who served most recently as a vice president. "You immediately had to get out there and perform, and if you didn't perform, you were cut."

Equifax's roots as a behind-the-scenes data collector stretch back to 1899, when it began as the Retail Credit Company. Grocers and other retailers kept notes on their customers to determine who could be trusted to run tabs and pay them. Two brothers in Atlanta went door to door to collect that information. They compiled it into a publication called "The Merchant's Guide" and sold annual subscriptions for $25.

The company and its competitors swept through the country, employing thousands of investigators to investigate people's lives. Their reports were widely available for sale to anyone except the individuals themselves.

In the 1960s, the credit bureaus' secrecy and unchecked power prompted alarm within Congress. The hearings that followed exposed the more unsavory practices, like including unverified gossip about people's marital indiscretions in their reports. The bureaus amassed personal dossiers so detailed that J. Edgar Hoover was covetous.

"The F.B.I. is constantly in our files," an executive at a credit bureau testified.

Congress responded by passing the Fair Credit Reporting Act, which created some safeguards. For the first time, people were allowed to review their own files and report errors.

But the strongest agencies just kept growing, often by acquiring rivals. By the late 1990s, three big national players were left.

With little competition, the bureaus saw an opening for a new sales market: capitalizing on consumers' curiosity and concern about their credit files.

In 2001, Equifax teamed up with Fair Isaac to let people buy their three-digit FICO credit scores. Today, Equifax charges people $40 to see all three of their reports. (Consumers are entitled to one free credit report from each of the bureaus annually.)

The company's consumer business generates $400 million in annual sales, much of it through resellers. Using Equifax data, LifeLock sells identity theft protection, a booming business since the breach.

Such sales, while strong, are eclipsed by the money Equifax makes from human resources products. It entered the market in 2007 with the purchase of Talx, which verified employment for companies.

Mr. Smith viewed Talx as a beachhead into a lucrative new data field: payroll information. When Equifax bought the company, Talx held 142 million employment records. The unit now has 300 million.

“It’s been a nearly 10-year investment, but now it’s paying off for Equifax,” said Brett Horn, an investment analyst at Morningstar. “They have something their rivals don’t.”

A few expansion efforts fizzled, especially in tightly regulated markets. In 1995, Equifax teamed with AT&T to develop health care products, including electronic patient records. The effort quietly died a year later, right around the time that Congress passed a strict medical privacy bill.

As the industry expanded, safety became a sales pitch. “We have been blessed in our rich history to never have a major breach,” Mr. Smith said at a financial conference shortly after joining the company in 2005.

In one document, Equifax called itself the “trusted stewards of data.”

“If you’re not ahead of security risk,” the pitch read, “you’re behind it.”

After previous smaller breaches, the bureaus have been reluctant to offer consumers the strongest form of protection, credit freezes, free of charge. Freezing a file prevents new credit lines from being opened, which locks out identity thieves.

After Experian’s servers were attacked two years ago, exposing personal details on 15 million T-Mobile customers, consumer advocates urged both companies to provide free credit freezes at all three bureaus.

Doing that would set a terrible precedent and “haunt” all future breaches, Experian’s senior vice president of government affairs and public policy said in a response intended for executives at his company and T-Mobile. The reply was accidentally emailed to one of the advocates.

Giving in to the demand “will not satiate their hatred for Experian,” he added. Instead, he suggested responding with a letter explaining why fraud alerts were good enough. “We could turn our response into a good P.R. approach if done right,” he wrote.

Experian said in a statement that the opinions in the email did not reflect the company’s position. The company said it had provided affected individuals with free credit monitoring and credit freezes at Experian at no charge.

Equifax’s own response to its breach has been marred by blunders.

An Equifax website was supposed to allow customers to determine if they had been affected; it didn’t work correctly. The company’s Twitter account accidentally steered people toward a fake site. And when millions of consumers went to freeze their Equifax credit files, some had to pay for the service. After people protested, the company waived the fees.

From a business perspective, it will be paramount for Equifax to keep its customers — financial firms and other big companies — happy.

Six of America’s largest financial services companies — American Express, Bank of America, Capital One, Citibank, Discover and JPMorgan Chase — declined to comment on whether the breach would alter their relationships with Equifax. Walmart, the nation’s largest private employer, and Kroger, the second biggest, said they were comfortable continuing to send Equifax their payroll data.

Still, some — mainly smaller organizations — are beginning to rethink their relationship with the company.

Summit Credit Union in Madison, Wis., filed a lawsuit against Equifax. The firm is seeking compensation for the economic harm that it said it was likely to suffer from the breach.

"This situation has caused us all to pause," said Sandi Papenfuhs, senior vice president of consumer lending at another firm, First Tech Federal Credit Union in Beaverton, Ore. "Anytime someone is not securing member data to the same degree that we do and we expect, we will take action on that relationship accordingly."

But her credit union will continue to send Equifax data. Withholding information would only hurt consumers, she explained, because it would create an incomplete picture of their credit history.

"I am unaware of a way to just stop, from any individual lender perspective," Ms. Papenfuhs said, "and not cause consumer harm."

Danny Hakim contributed reporting.

A version of this article appears in print on September 24, 2017, on Page A1 of the New York edition with the headline: Equifax Made Shielding Data Part of Sales Pitch.
