Equifax says it had a security breach earlier in the year

19 September 2017, by Ken Sweet

This Saturday, July 21, 2012, photo shows the corporate headquarters of Equifax Inc. in Atlanta. New York Attorney General Eric Schneiderman is pressing credit monitoring companies TransUnion and Experian to explain what cybersecurity they have in place to protect sensitive consumer information following a breach at Equifax, discovered by the company in July 2017, that exposed the data of 143 million Americans. (AP Photo/Mike Stewart)

Equifax, under pressure from a massive data breach, says it had a separate incident earlier this year. That may mean even more scrutiny as the company deals with the aftermath of a security failure that exposed the information of 143 million Americans.

Meanwhile, the Massachusetts Attorney General has filed suit against Equifax. And Equifax says about 100,000 Canadian consumers may have had their personal information compromised.

Here's the latest on the breach:

AN EARLIER BREACH

Equifax says it had a security breach earlier this year that involved a different part of the company than the one accessed in the larger hack.

The breach involved TALX, which is Equifax's human resources and payroll service. The company said there's no evidence that the TALX breach, which happened between March and April this year, and the wider breach are related.

The TALX breach, which at the time was relatively minor, is likely to attract additional scrutiny.

Three executives at Equifax were found to have sold stock in the days leading up to the time when Equifax disclosed the more serious breach. Equifax says the three executives, which includes the company's second-highest ranking employee, its chief financial officer, were unaware of the bigger breach when they sold their shares.

Equifax hired the same cybersecurity company, Mandiant, to handle both breach investigations.

STATE ACTION

Massachusetts Attorney General Maura Healey sued Equifax on Tuesday, making it the first state to take direct legal action against the company following the breach. Its lawyers say that Equifax's negligence exposed more than half the state's adult population to the breach, and the company was negligent in dealing with security threats, including the software vulnerability that has become the center of the investigation.

Attorney General Healey is seeking unspecified civil penalties, restitution and damages for the impacted residents.

TRANSUNION AND EXPERIAN NOW UNDER STRUTINY

New York Attorney General Eric Schneiderman is questioning two other credit-monitoring companies,

TransUnion and Experian, about what precautions they have taken to protect sensitive consumer information. In letters to company executives, the Democratic attorney general asked them to describe their existing security systems, as well as what changes they've made since the Equifax hack.

This Saturday, July 21, 2012, photo shows signage at the corporate headquarters of Equifax Inc. in Atlanta. New York Attorney General Eric Schneiderman is pressing credit monitoring companies TransUnion and Experian to explain what cybersecurity they have in place to protect sensitive consumer information following a breach at Equifax, discovered by the company in July 2017, that exposed the data of 143 million Americans. (AP Photo/Mike Stewart)

The breach, he wrote, "has raised serious concerns about the security of private consumer information held by the nation's largest consumer credit reporting agencies." The letters also ask whether the companies are considering waiving the fees for consumer credit freezes. The costs of those vary by state. .

CANADIAN TALLY

Equifax said Tuesday that approximately 100,000 Canadian consumers may have had personal information breached, including names, addresses, social insurance numbers and in some cases credit card numbers.

Equifax Canada's president and general manager Lisa Nelson apologized to consumers whose data may have been compromised. The company says the investigation is still going on.

Canada's privacy watchdog has said it is looking into the breach and Equifax has committed to notifying those affected in writing as soon as possible.

WHAT IS EQUIFAX DOING?

Equifax's CEO has been called to testify before Congress on Oct. 3, and the company announced last week that its chief information officer and chief security officer would be leaving the company immediately. It also has bulked up its call centers and is waiving fees for credit freezes.

The credit data company also released a detailed, if still muddled, timeline of how it discovered and handled the breach.

Equifax's stock has fallen more than a third since the scandal broke.

WHAT SHOULD I DO?

Consumers should be vigilant and diligent. That means:

— Closely monitoring their credit reports, which are available free once a year, and stagger them to see one every four months.

— Keeping watch, possibly for a long time. Scammers who get ahold of the data could use it at any time—and with 143 million to choose from, they may be patient.

— Considering freezing your credit reports. That stops thieves from opening new credit cards or loans in your name, but it also prevents you from opening new accounts. So if you want to apply for something, you need to lift the freeze a few days beforehand.