New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 57
THURSDAY, SEPTEMBER 21, 2017

Lawyers Say More Regulation Is Likely to Follow Equifax Breach

BY JOSEFA VELASQUEZ

FOLLOWING the Equifax data breach, lawyers are pondering what new regulations, if any, will come out of the massive cyberattack that compromised sensitive information of 143 million Americans.

Steven Kuperschmid, a partner at Ruskin Moscou Faltischek in Uniondale who chairs the firm's corporate and securities department, anticipates that the federal government will issue broad new regulations on cybersecurity following this event.

Steven Kuperschmid

Nicole Della Ragione

"I think there will be a broadening of the regulations and potentially uniform regulations proposed on the federal level. I don't think that's going to happen overnight," Kuperschmid told the New York Law Journal in an interview Tuesday afternoon.

Because cybersecurity is still a developing area, laws governing it are more often reactive, Kuperschmid said. A prime example is New York's cybersecurity regulations governing banks and insurers, which recently took effect. The regulations, billed as first in the nation, require banking and insurance companies regulated by the state Department of Financial Services to comply with a new set of rules in an effort to prevent and mitigate cyberattacks. The rules require banks and insurance companies operating in the state to have state-approved plans to deter hacks and report them within 72 hours of when a data breach is suspected.

As the New York Law Journal reported earlier this month, the cybersecurity regulations didn't apply to the credit reporting agencies (NYLJ Sept. 8). In New York, Gov. Andrew Cuomo is looking to change that.

On Monday, the Democratic governor proposed new regulations that would subject credit reporting agencies to the same cybersecurity rules as the banking and insurance industry (NYLJ Sept. 18). Under those rules, credit reporting agencies such as Equifax, TransUnion and Experian would have to register with the state Department of Financial Services starting in February and every year thereafter. Their registration form would also have to include the agency's officers or directors who would be responsible for compliance with the recently enacted cybersecurity regulations.

If credit reporting agencies don't comply with the regulations proposed by the governor, then state-regulated entities, such as banks, would not be able to use noncompliant companies for credit reports, said Mayer Brown partner Jeff Taft, who is a financial services regulatory lawyer specializing in

banking, consumer financial services and cybersecurity.

"If you don't want to comply with New York's requirements, New York is telling its regulated entities that they can't use you to provide credit reports and you can't provide credit reports on people located in New York," Taft said in an interview.

The senior vice president of public policy and legal affairs at the Consumer Data Industry Association said the trade group, which represents credit bureaus, is still reviewing the regulations issued in New York. "We are reviewing the proposal, but we're not prepared to comment at this time, as our focus is on cybersecurity and supporting consumers potentially affected by the cyberattack," said Eric Ellman in an emailed statement.

While New York is the first to issue such regulations regarding cybersecurity, it won't be the last Taft said.

"I think it's very difficult at a federal level to propose cybersecurity regulations that apply without regard to industry," said Taft, who later added that the Equifax breach could reignite the conversation about data breach disclosures at the federal level.

In 2016, three banking regulatory agencies had issued an advanced notice of proposed federal rulemaking for cyber risk management standards for financial institutions but its future is unclear under the Trump administration, leaving the New York rules, which apply to banks and insurers that do business in New York regardless of where they originate, among the most comprehensive laws in the United States for financial services related data at the moment. California also enacted stricter laws for data breach disclosure by all types of businesses in 2016. California had among the earliest data breach notification laws, dating back to 2003.

According to New York Attorney General Eric Schneiderman's office, which is investigating Equifax over the security breach (NYLJ Sept. 8), the hack may have compromised sensitive information—including Social Security numbers, birthdays, addresses and driver's license numbers—of 8 million people in New ork.

While the attorney general in New York continues to investigate the cause of the massive breach at Equifax, his office has sent formal inquiries to two major credit reporting agencies to inquire about their data security. In a letter to the CEOs of Experian and TransUnion sent last week, Schneiderman is seeking information about their security protocols before they learned of the Equifax breach and steps the companies have taken in the weeks following the Sept. 7 breach to protect customer information.

On Monday, Massachusetts Attorney General Maura Healey filed the first enforcement action in the United States against Equifax, according to her office, over the company's alleged failure to protect the personal and sensitive information on nearly 3 million Massachusetts residents.

"We allege that Equifax knew about the vulnerabilities in its system for months, but utterly failed to keep the personal information of nearly three million Massachusetts residents safe from hackers," said AG Healey. "We are suing because Equifax needs to pay for its mistakes, make our residents whole, and fix the problem so it never happens again."

Like New York's Schneiderman, Healey's office also launched an investigation of the credit bureau. She announced her intent to sue Equifax last week and filed a complaint seeking a jury trial in Suffolk County court in Massachusetts on Sept. 19.

In a rare move, the Federal Trade Commission also acknowledged that it has launched an investigation of the breach.

In the meantime, companies should actively keep up with security actions and make the required patches, said Nicole Della Ragione, an associate at Ruskin Moscou Faltischek and member of the firm's cybersecurity and data privacy practice group.

@ Josefa Velasquez at jvelasquez@alm.com; Twitter: @J__Velasquez.