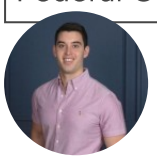
NEWS

Data-Breach Class Actions Surge Across US Federal Courts in Prior 12 Months

"A year from now, we will be looking back at this data and thinking about the good ol' days when only 33 cases per month were considered low,'" said Franklin Zemel, who co-chairs the first U.S. standing committee on cybersecurity and privacy law for the Florida Bar.

July 12, 2023 at 03:54 PM

Federal Government



Michael A. Mora

What You Need to Know

- There has been a 154% increase in the last year in federal data breach class actions.
- The pre-trend lawsuit average was 13 per month and has surged to 33 per month, with the number since rising in July.
- An expert said that notably when an attack has occurred, federal courts are finding that post-indictment assessments may not be privileged.

In June, plaintiffs attorneys filed more than 60 federal data breach class actions, a surge that is part of an overall trend over the last year, in which there have been an average of 33 of these suits per month, well above the 13-suit average in the 12 months prior to that, per Law.com Trend Detection.

“A year from now, we will be looking back at this data and thinking about the good ol’ days when only 33 cases per month were considered low,’” said Franklin Zemel, a Saul Ewing partner in Fort Lauderdale. Zemel co-chairs the first U.S. standing committee on cybersecurity and privacy law for the Florida Bar, in part, to counter the prevalence and impact of data breaches.

“Businesses must undertake an appropriate assessment of current security standards,” Zemel said. “I recommend that businesses engage appropriate legal counsel to serve as the point for such an assessment because it provides attorney-client and work product privileges to that process. Notably, once an attack has occurred, courts are finding that post-incident assessments may not be privileged.”

So far, there has been a 154% increase from the pre-trend average, with now over 399 cases in the U.S. District Court for the Southern District of Florida, and in federal jurisdictions in New York, California, Texas, Pennsylvania, and over a dozen additional states.

And law firms are not immune from becoming a prime target of data breaches, as reported by the American Lawyer.

Related story: Class Action Lawsuit Hits Bryan Cave After Data Breach

In June, a former employee of snack-food maker Mondelez sued Bryan Cave with a class action lawsuit in the Northern District of Illinois, alleging implied contract, breach of contract, unjust enrichment, and invasion of privacy. The plaintiff's personal data, as well as the data of more than 51,000 additional former and current employees, was hacked from Bryan Cave's computers in late February.

The data breaches concept began well before computing when a person physically accessed a record without authorization.

Still, in the 1980s, computers developed to where publicly disclosed data breaches increased frequently, prompting new laws and regulations, per cybersecurity provider Fortra. And starting in 2005, technology reached a point at which it connected globally, providing bad actors an opening.

Nowadays, a common claim in these lawsuits is that companies had advance notice of the hacking risk, and therefore, should have been able to protect their user data. For instance, Milberg Coleman filed a data breach class action Monday in the U.S. District Court for the Northern District of Ohio against health care revenue cycle company Intellihartx LLC.

The Am Law 100 firm sued the health care company over its alleged failure to implement adequate data security measures stemming from a February breach of approximately 489,000 class members. And the plaintiff's attorneys argued in the complaint that the defendant should have prevented the data breach.

Here, there was an example that data breaches "targeting healthcare entities that collect and store private information" have become "so notorious" that the FBI and the U.S. Secret Service "have issued a warning to potential targets so they are aware

of, and prepared for, a potential attack." The lawsuit cited at least a half-dozen leading entities.

Moving forward, Zemel, the Florida Bar expert, warned of "substantial increases in these industry-specific attacks," even beyond health care, such as in the insurance, military, consulting and research sectors. At the same time, corresponding attorney fees could incentivize the surge in lawsuit filings and some quick settlements, but Zemel warned against a broad generalization.

"Ultimately, the class plaintiffs' lawyers will look to be paid a percentage of the value of the benefits obtained in either a class action settlement or judgment," Zemel said. "And to the extent that some, but not all class litigation, changes thinking and forces behavioral changes, it can provide overall benefits with respect to how we all think and act about cybersecurity."

Read the complaint: