Trial®

TOP STORY

LAWSUITS MOUNT AGAINST EQUIFAX AS JUDGE RULES YAHOO MUST FACE CYBERSECURITY CLASS ACTION

October 2017 - Diane M. Zhang

The fallout from two high-profile security breaches has underscored ongoing concerns over the safety of sensitive consumer information in the hands of large corporations. In early September, Equifax—one of the nation's largest credit reporting agencies—revealed that it had discovered a massive security breach in July that compromised the Social Security numbers, addresses, birthdays, and driver's license numbers of nearly 143 million people. And on Aug. 30, a federal district court ruled that Yahoo will have to face a consolidated class action that was filed after the company disclosed a series of security breaches that compromised the accounts of more than 1 billion customers.

The fallout from two high-profile security breaches has underscored ongoing concerns over the safety of sensitive consumer information in the hands of large corporations. In early September, Equifax—one of the nation's largest credit reporting agencies—revealed that it had discovered a massive security breach in July that compromised the Social Security numbers, addresses, birthdays, and driver's license numbers of nearly 143 million people. And on Aug. 30, Judge Lucy Koh of the Northern District of California ruled that Yahoo will have to face a consolidated class action that was filed after the company disclosed a series of security breaches that

compromised the accounts of more than 1 billion customers. (*In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017).)

On July 29, Equifax discovered that some of its servers—which contained consumers' sensitive personal information—had been hacked by an unknown party. The credit reporting company monitored network traffic, and an internal review discovered a vulnerability in one of its web application frameworks. Equifax contacted a cybersecurity firm to conduct a forensic review of the breach, but it did not disclose the cyberattack until several weeks after its initial discovery. Soon after, it was revealed that multiple Equifax executives had sold shares of their company stock in early August—only a few days after the breach was discovered internally. Consumers, however, learned of the breach only when news broke publicly.

Chicago attorney Kenneth Lumb, who filed a class action in the Northern District of Illinois on behalf of consumers nationwide whose personal data was collected and stored by Equifax, emphasized the sensitivity of the stolen information. (*Meyers v. Equifax Info. Servs., LLC*, 1:17-cv-06652 (N.D. Ill. filed Sept. 14, 2017). "The information stolen includes names, addresses, Social Security numbers, credit and payment histories, and even credit card numbers—in short, all of the information necessary to steal an identity, open accounts, and apply for credit cards and other forms of credit in the individual's name," he explained.

The complaint alleges that Equifax failed to implement reasonable procedures to protect the plaintiffs and failed to timely notify or warn consumers of the breach. "Equifax's decision to wait six weeks after the breach before informing all consumers was willful and wanton, as well as negligent," the complaint reads. "By depriving the plaintiffs and class members of information about the breach in a timely manner, Equifax subjected each consumer to a concrete information injury, as these consumers were deprived of an opportunity to meaningfully consider and address issues related to the potential fraud."

The lawsuit alleges that Equifax was negligent in handling and protecting the sensitive information. "The standard of care is defined by what a reasonably careful company would do to safeguard extremely sensitive information," Lumb said. He noted that Equifax had been aware of the bug before the breach happened. "The developer of the software discovered the bug and provided a patch to Equifax in March—but Equifax did nothing," Lumb said.

He added, "This is only the tip of the iceberg."

The class action is one of dozens that are steadily increasing across the country. Individuals are no longer the only ones suing the credit reporting company—small businesses are also seeking damages for financial losses resulting from the cyberattack. Among them is a Sept. 20 class action filed in the Northern District of Georgia by three businesses claiming that the breach could negatively impact their ability to secure loans or lines of credit. (*O'Dell Props., LLC v. Equifax, Inc.*, 1:17-CV-03618 (N.D. Ga. filed Sept. 19, 2017).)

A decision last August from the Northern District of California is also likely to facilitate lawsuits against companies for cyberattacks. Yahoo, which suffered a series of attacks affecting more than 1 billion users between 2013 and 2016, similarly did not immediately disclose the security breach to their customers—waiting years after the first known security incident to inform impacted consumers. The consolidated class action against the company, which combines 12 different plaintiffs' originally separate claims, seeks damages from Yahoo for exposing personally identifiable information associated with their user accounts, including zip codes, passwords, cell phone numbers, and addresses.

The class action, which was consolidated in December 2016, alleges that Yahoo had been put on notice due to its long history of data security failures over a decade and had been negligent in handling and resolving vulnerabilities in its cybersecurity systems. Yahoo, however, moved to dismiss the class action, arguing that the plaintiffs lacked Article III standing—which requires that plaintiffs suffer an injury-in-fact that is concrete and

particularized and actual or imminent, “fairly traceable” to the challenged conduct, and likely to be redressed through a favorable decision.

Judge Lucy Koh rejected Yahoo’s argument, ruling that all plaintiffs had adequately alleged an injury-in-fact sufficient for Article III standing “because all Plaintiffs have alleged a risk of future identity theft.” The judge also noted that some plaintiffs had spent money to protect themselves from future identity theft and that some plaintiffs had already experienced misuse of their personal information by identity thieves—for example, two plaintiffs alleged that their Social Security numbers had been stolen from their Yahoo email accounts.

Koh also rejected Yahoo’s argument that the company had not itself collected sensitive data. Because some plaintiffs had used or included personal identifying information while logged into their Yahoo accounts, the company argued, the alleged harm was a result of the plaintiffs’ activities—not Yahoo’s. Koh, however, responded that this was not persuasive. She also pointed to the plaintiffs’ allegations that the defendant’s lax security practices allowed hackers to continually access their Yahoo accounts.

Notably, Yahoo did not disclose the series of security breaches until September 2016, two months after it announced Verizon’s plan to acquire its operating assets—and weeks after it reported to the U.S. Securities and Exchange Commission that it was unaware of any incidents of unauthorized access of data that could adversely affect the acquisition. The plaintiffs alleged that this was financially motivated: Yahoo solicited offers from potential buyers until April 2016. Verizon completed its purchase of Yahoo for $4.48 billion last June, down from the previously announced purchase price of $4.83.

777 6TH STREET, NW, SUITE 200 WASHINGTON, DC 20001

800.424.2725 | 202.965.3500