

Yahoo tries to settle 3-billion-account data breach with \$118 million payout



Enlarge / A Yahoo logo on a smartphone.
Getty Images | SOPA Images

reader comments

51 with 40 posters participating

Share this story

Yahoo and plaintiffs, in a case over a data breach affecting three billion user accounts, have agreed to a settlement that would require Yahoo to pay \$117.5 million.

The sides previously agreed to a settlement of \$50 million plus attorneys' fees and other expenses, but it was rejected by US District Judge Lucy Koh in January.

Yahoo and the plaintiffs filed their new proposed settlement yesterday in US District Court for the Northern District of California. This one will also face a judge's review.

"Following the Court's denial of [the first proposed settlement], the Parties immediately set about addressing the issues the Court identified, re-engineering the resolution of this case," the new proposal says. "The Amended Settlement Agreement not only provides the biggest common fund ever obtained in a data breach case (\$117,500,000.00), it materially moves the benchmarks on: The individual claim cap (\$25,000), the amount of lost time that can be reimbursed (15 hours), the minimum rate at which such time is compensated (\$25.00/hour), and alternative compensation for those already having credit monitoring (\$100, up to full retail value of \$358.80)."

The \$117.5 million would pay for the following:

- *At least two years of credit monitoring, open to all Class Members without any cap as to the number of potential claimants, at a cost of \$24 million*
- *Notice and administration costs of no more than \$6 million*
- *Attorneys' fees of no more than \$30 million and costs and expenses of no more than \$2.5 million*
- *Service awards of between \$7,500 and \$2,500 per Settlement Class Representative*
- *Alternative compensation of \$100 for those individuals already having credit monitoring*
- *Out-of-pocket expenses related to identity theft, lost time, paid user costs, and small business user costs*

The proposed settlement class would include all US and Israeli residents and small businesses with Yahoo accounts at any time between 2012 and 2016. That includes at most 896 million accounts and 194 million people.

The 2013 data breach affected all three billion Yahoo user accounts worldwide, including about one billion accounts in the US and Israel. An attempt to include plaintiffs from Australia, Venezuela, and Spain in the case was previously rejected by the court. The lawsuit also covers two other data breaches, one in 2014 and another in 2016.

“According to Plaintiffs, Defendants did not use appropriate safeguards to protect users’ personal identification information (‘PII’), and Plaintiffs’ PII was thus exposed to hackers who infiltrated Defendants’ systems,” Koh noted in her January ruling. “Moreover, Plaintiffs allege that Yahoo ‘made a conscious and deliberate decision not to alert any of Yahoo’s customers that their PII had been stolen.’”

Yahoo disclosed in October 2017 that the 2013 breach affected three billion accounts, every single one that existed at the time. Before that, Yahoo had said one billion accounts were compromised. As we previously reported, information taken in the heist may have included users’ names, e-mail addresses, telephone numbers, dates of birth, passwords scrambled using the weak MD5 cryptographic hashing algorithm, and, in some cases, encrypted or unencrypted security questions and answers. Yahoo says that “an unauthorized party stole data” and that “all accounts that existed at the time of the August 2013 theft were likely affected.”

Yahoo was acquired by Verizon in June 2017.

Why the first settlement was

rejected

Koh's January ruling said the proposal inadequately disclosed the size of the settlement fund, the scope of non-monetary relief, and the size of the settlement class.

The original settlement included "\$50 million to cover out-of-pocket costs, alternative compensation, paid user costs, and small business user costs," Koh's ruling said. However, "[t]he proposed notice does not disclose the costs of credit monitoring services or costs for class notice and settlement administration, and does not disclose the total size of the settlement fund," Koh wrote. "Without knowing the total size of the settlement fund, class members cannot assess the reasonableness of the settlement."

The total size of the settlement fund would have been larger than \$50 million because the settlement separately would have provided for "attorneys' fees of up to \$35 million, costs and expenses of up to \$2.5 million, and service awards of up to \$7,500 each for settlement class representatives."

But it wasn't clear that all of the \$35 million was needed for attorneys' fees, so much of that \$35 million could have thus gone back to Yahoo, "reduc[ing] the total amount that Yahoo would have to pay as a result of the settlement" and preventing the court and class members from assessing the reasonableness of the settlement, Koh wrote at the time.

"The only numbers to which the parties commit in the settlement agreement, motion for preliminary approval, and proposed notice are \$50 million for the settlement fund, up to \$35 million in attorneys' fees, and up to \$2.5 million in attorneys' costs and expenses, for a total of \$87.5 million," Koh's January ruling said. "Based on these numbers, attorneys' fees would be 40 percent of the settlement fund. Taking account of the additional funds the parties disclosed under seal in their supplemental filing, the Court finds that the

attorneys' fees request remains much greater than the 25 percent benchmark standard used in this Circuit."

Koh also faulted Yahoo for failing to commit to specific increases in its security budget.

Un-awarded attorneys' fees will go to victims

In the new proposed settlement, any unclaimed attorneys' fees would remain in the settlement fund for dispersal to class members.

Yahoo also committed to "maintain an information security budget of more than \$300 million over the next four years and a team headcount of 200, amounts that are at least four times and three times greater, respectively, than Yahoo maintained prior to this case."

Plaintiffs asked the court to find that the new settlement agreement is "fair, reasonable, and adequate."

Yahoo has settled several other lawsuits related to the data breaches, including a \$35 million settlement with the Securities and Exchange Commission for misleading investors by failing to disclose the data breaches; \$80 million in a federal securities class action related to Yahoo's failure to disclose the data breaches; and a \$29 million settlement in a shareholder class action.

<https://arstechnica.com/?p=1489317>