

Cybersecurity & Privacy Group Of The Year: Robbins Geller

By **Ben Kochman**

Law360 (December 10, 2020, 3:49 PM EST) -- Robbins Geller Rudman & Dowd LLP helped win initial approval of a \$650 million, all-cash settlement on behalf of Illinois residents bringing biometric privacy claims against Facebook, landing the firm a place among Law360's 2020 Cybersecurity & Privacy Groups of the Year.

The California-based plaintiffs firm, along with co-counsel at Labaton Sucharow LLP and Edelson PC, struck a deal with Facebook in January, on the eve of a trial that could have exposed Facebook to billions of dollars in damages if the tech giant was found to have violated Illinois' Biometric Information Privacy Act with its face-scanning "tag" suggestion feature.

More than 1.5 million Illinois Facebook users have sought to claim a share of the settlement fund that received preliminary approval in August, according to filings in the case. Class counsel has projected that claimants will receive between \$200 and \$400 in cash, with Facebook also agreeing to set users' face recognition settings to "off" by default and to delete class members' stored face templates unless the company first gets consent to use them.

Plaintiffs' attorneys were able to secure the largest cash-only settlement in the history of U.S. privacy class actions by simultaneously negotiating behind the scenes with Facebook while being prepared to take the case all the way to a jury, said Paul Geller, one of the firm's founding members.

"We could have settled this case early on for what I call 'window dressing,' but the reason we were able to get this type of development is that we were willing to get this case to trial," Geller said.

Notably, the entire settlement fund is devoted to cash payouts for Facebook users — regardless of whether they can show that they've suffered a specific harm beyond the tech giant's alleged use of their facial geometry without first getting consent.

The fund's structure differs from the arrangement worked out in the Equifax data breach litigation, for example, which a Georgia federal court approved in December 2019.

A \$300 million restitution pool set aside for members of that class was mostly devoted to paying for



credit monitoring services or to claimants who could show documented losses related to the breach. Just \$31 million was set aside specifically for cash payouts, despite overwhelming interest that breach victims had originally shown in a previously announced \$125 cash option.

"One of the hallmarks of our group is that we try to recover real money, and get real results," said Geller of the Facebook deal, adding that, "I hope the days of a credit monitoring settlement are behind us."

The preliminary settlement approval in the Facebook case came after a California federal judge rejected a previous \$550 million version of the deal. Class counsel are seeking \$110 million in fees and expenses.

The case would have been the first-ever BIPA lawsuit to go to trial, and both sides had expected to grapple with unprecedented questions facing a jury, including whether Facebook users had in fact "consented" to the company's practices at issue.

"We were going to be trying a case that didn't look like any case that has been tried before," said Shawn Williams, managing partner of Robbins Geller's San Francisco office, who led the firm's trial preparation efforts.

Privacy and data breach cases in general have steadily become a larger part of Robbins Geller's practice in recent years, with roughly two dozen attorneys out of a total of around 200 in the firm working full-time on such cases, Geller said.

Beyond the Facebook case, the firm is also on the executive committee of plaintiffs' firms representing consumers in a \$117.5 million deal approved in July, which resolved multidistrict litigation involving 194 million class members over Yahoo's multiple data breaches.

Geller says the firm expects to file more and more cases in the area as more and more privacy concerns arise, including the threat of consumers' geolocation data being misused. Facial recognition technology, which researchers have found to have disproportionately higher false positive rates for Black, Asian and Native American people, has also drawn criticism from privacy advocates calling for it to be outlawed or tightly regulated.

"Clearly, these kinds of data privacy cases are a growing trend in the future of class action litigation," said Geller. "We turn away more than we file."

--Editing by Bruce Goldman.