LinkedIn Ruling Boosts Prospects For Data Breach Plaintiffs

By Allison Grande 0 Comments Share us on:

Law360, New York (April 15, 2014, 2:15 PM ET) -- A California federal judge recently allowed a putative class action over LinkedIn Corp.'s 2012 data breach to proceed based on allegations that the site made security misrepresentations in its privacy policy, endorsing a new strategy sure to become even more popular with plaintiffs attorneys stymied by standing hurdles in breach suits.

In a March 28 ruling rejecting LinkedIn's motion to dismiss the suit, U.S. District Judge Edward Davila concluded that lead plaintiff Khaliah Wright had on her third attempt met the standing requirements to bring claims under California's Unfair Competition Law by asserting that she had read and based her decision to purchase a premium account on the site's allegedly misleading privacy policy representations.

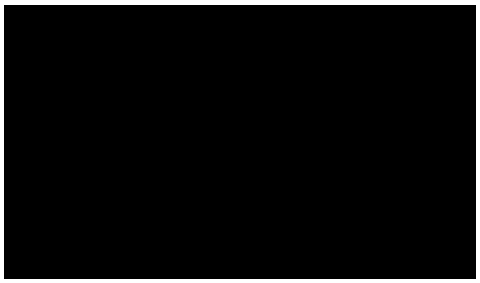
The judge's decision to allow the case to proceed by declining to treat privacy policy misrepresentations differently from misleading labels marked a rare victory for the plaintiffs' bar, which often struggles to get past the motion to dismiss stage in breach cases in which the plaintiffs are unable to show that the intrusion led to the misuse of their personal or financial data, according to attorneys.

“Although in the past, plaintiffs in data breach cases may have struggled to meet Article III standing requirements, this case is yet another example of where these plaintiffs appear to be gaining ground,” Fox Rothschild LLP attorney Amy Purcell said. “By permitting the analogy between a company's privacy policy and a product's labeling or advertising, the court has provided these already creative plaintiffs with a new and additional argument to use to overcome the standing hurdle.”

With companies reporting data breaches more regularly than ever before, plaintiffs' class action attorneys have been busy in recent years filing suits seeking to recoup damages and hold companies liable for failing to adequately secure the sensitive data that they hold.

After discovering that courts were less than receptive to the argument that the threat of data misuse was enough to establish standing, plaintiffs began to turn to more creative theories, including that consumers had been misled about the level of security that companies had employed to protect the personal data with which they had been entrusted.

Mark Melodia, who leads Reed Smith LLP's global data security, privacy and management practice, noted that plaintiffs have been pushing a set of liability and damages theories based on consumer fraud, false advertising and unjust enrichment “at least since the first round of motions” in litigation over the 2011 Sony PlayStation data breach, and attorneys say that the LinkedIn ruling shows that their persistence and creativity are beginning to pay off.



Related

Sections

- California
- Class Action
- Consumer Protection
- Corporate
- Media & Entertainment
- Privacy

Case Information

Case Title

TRACK Szpyrka v. Linkedin Corporation

Case Number

5:12-cv-03088

Court

California Nor hern

Nature of Suit

Other Statutory Actions

Judge

Edward J. Davila

Date Filed

June 15, 2012

Law Firms

TRACK Alston & Bird
TRACK Cooley LLP
TRACK Edelson PC
TRACK Fox Rothschild
TRACK Kaplan Fox
TRACK Morris Polich
TRACK Reed Smith
TRACK Siprut PC

Companies

TRACK LinkedIn Corp.

“The court’s decision to allow the plaintiff’s unfair competition law claims to proceed is at this point a testament to artful pleading on the plaintiff’s part to ensure all of the requisite elements of the claim have been pleaded,” said Torin A. Dorros, the managing attorney of Los Angeles-based boutique firm Dorros Law.

Given that companies are increasingly inserting assurances about the strength of their data security into privacy policies as consumers become more attuned to the issue, the theory endorsed by Judge Davila's ruling is likely to become an enticing hook for the plaintiffs' bar, according to attorneys.

“This is a good case for privacy plaintiffs in that it takes a broad view of the types of statements that can support these types of unfair competition claims,” said Venkat Balasubramani, a partner with Internet and media boutique Focal PLLC.

While attorneys expect the most action to come out of California, due to the strength of the unfair competition law statute and the general sense that the state is more open to privacy claims than other jurisdictions, attorneys didn't discount the possibility that the argument could spread to other states with similar false labeling restrictions.

“Whether other jurisdictions will similarly pick up on it or not is still an open question, but it would not be surprising to see an argument that works in one jurisdiction spreading,” Melodia said.

In light of the risk posed by the standing theory boost, companies would be wise to carefully consider the significance of each and every word in their privacy policies and ensure that they are living up to those words, according to attorneys.

“Companies need to keep in mind that what they have in their privacy policy may very well find its way into a suit as a basis for alleged standing, so it's important to keep a close eye on data security practices so that when certain buzzwords such as 'industry standard' are used, they are accurate,” Alston & Bird LLP partner Dominique Shelton said.

The task is even more vital in the current privacy environment, where no general data security legislation or other overriding agreement defines what actually constitutes “reasonable” or “industry standard” practices.

“'Reasonableness' is a plaintiffs' friend,” Balasubramani said. “At the motion to dismiss stage, even a vague standard like reasonableness could be enough of a hook for a plaintiff, so when a company makes a statement like that, they need to be thinking about the implications.”

Companies' best bet may be to say that they “do their best” to protect security or make other more general statements that avoid assertions that “can open up a company to exposure when it is discovered, as alleged here, that it didn't follow such a standard,” said Morris Polich & Purdy LLP cyber, privacy and data security practice head Timothy Toohey.

But while the LinkedIn ruling seemingly opens a new door for the plaintiffs' bar, the forecast isn't entirely bleak for companies, according to attorneys.

"While this creative use of false advertising theories has allowed the case to survive a Rule 12(b)(1) motion, it is highly questionable as a long-term strategy for plaintiffs' class action counsel," Melodia said.

For one, plaintiffs are likely to have difficulty maintaining their claims at later stages in the litigation, when they will have to find facts to support their allegations, unlike at the motion to dismiss stage, when the court must accept their allegations as true, according to attorneys.

Class certification is likely to be a significant hurdle for plaintiffs as well, given that it likely will require individualized proof that each potential class member read and relied on LinkedIn's allegedly false statements.

"At worst, a decision like LinkedIn means that corporate defendants will shift their attention to winning these cases on summary judgment and, particularly, on class certification," Melodia said.

The application of the theory is also likely to be limited to cases in which consumers paid for a service, given that users of free services would have a difficult time proving that the company's alleged security failures and misrepresentations caused them to lose anything valuable, attorneys noted.

"Companies who provide a free service won't get a pass, but they will have less to worry about because these types of unfair competition claims will not be easy to bring against companies that offer their services for free," Balasubramani said.

LinkedIn is represented by Michael G. Rhodes, Matthew D. Brown, Benjamin H. Kleine and Kathlyn A. Querubin of Cooley LLP.

The plaintiffs are represented by Jay Edelson, Rafey S. Balabanian, Ari J. Scharg and Christopher L. Dore of Edelson PC, Laurence D. King and Linda M. Fong of Kaplan Fox & Kilsheimer LLP, Joseph J. Siprut of Siprut PC, David C. Parisi of Parisi & Havens LLP and Dan Marovitch of Marovitch Law Firm LLC.

The case is In re: LinkedIn User Privacy Litigation, case number 5:12-cv-03088, in the U.S. District Court for the Northern District of California.

--Editing by John Quinn and Richard McVay.

Related Articles

LinkedIn Can't Escape Suit Over Password Hacking
LinkedIn Claims Lack Of Security Promise Dooms Breach Suit
Privacy MVP: Reed Smith's Mark Melodia
LinkedIn Says Stolen Passwords Didn't Cause Plaintiffs Harm