Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Blue Cross Can't Shake Data Breach Claims, Customers Say

By **Shayna Posses**

Law360, New York (July 15, 2016, 2:22 PM ET) -- The Blue Cross Blue Shield Association can't escape consolidated actions over a breach of health insurance data, customers argued Thursday in New York federal court, saying the company must be held responsible for failing to protect sensitive information.

The customers blasted BCBSA's bid to shake litigation over a data breach at Excellus BlueCross BlueShield, one of its licensees, contending that the company signed a contract promising federal workers health care and saying it would make sure the information consumers provided was protected. BCBSA broke that promise and now "seeks to elude responsibility for failing to discharge its contractual duties," the customers said.

"Notably, the motion to dismiss filed by BCBSA does not even attempt to demonstrate it held up its end of the bargain," they said. "Instead, it seeks refuge in hypertechnical, meritless defenses."

The lawsuits began after Excellus and its parent company, Lifetime Healthcare Inc., revealed on Sept. 9 that hackers had accessed records of roughly 10 million customers. The companies said the breach began in December 2013 and might have involved names, birthdates, Social Security numbers, mailing addresses, phone numbers, member identification numbers, financial account information and claims information.

The proposed class actions allege that the companies failed to protect customer information, waited too long to tell customers about the breach and did not give customers adequate information about how to protect themselves in the wake of the breach.

The customers also name BCBSA, a federation of 36 health insurance organizations and companies that provide insurance to more than 106 million people, according to the April consolidated master complaint. The allegations against the company stem from its contract with the Office of Personnel Management to sponsor and administer a federally sponsored health plan for federal employees, according to the customers.

BCBSA moved to toss the claims against it last month, arguing that it merely entered into the contract on behalf of independent insurance companies that it licenses the Blue Cross and Blue Shield marks to.

"BCBSA is not an insurance company and is not a parent, subsidiary, or sibling of any of the other defendants," the company said. "Its information systems were not attacked and it has no responsibility over the systems that were."

In addition, the company contended that the customers aren't entitled to sue to enforce the government's contract and that their claim under the New York General Business Law fails for a number of reasons, including the failure to adequately plead any violation.

However, the customers countered Thursday that Nina Mottern, one of the named plaintiffs, has the right to enforce the contract, under which BCBSA promised to provide the enrollees with data security safeguards. Under the Restatement of Contracts and federal common law, a contract can

be enforced by either a party to the agreement or an intended third-party beneficiary, the customers said.

Not only did BCBSA and OPM intend to benefit employees like Mottern, but they provided the federal workers with methods to enforce their rights, including an administrative procedure, according to the opposition brief.

The customers also argued that Mottern — and the federal employee class she seeks to represent — has standing to bring the claims because premiums were deducted from her paycheck for data security safeguards that she did not receive.

Finally, BCBSA's challenge to the New York General Business Law allegation fails as well, the customers said, contending that they sufficiently alleged misleading conduct that injured consumers and thus fulfilled the requirements for a deceptive business practices claim.

Hadley L. Matarazzo, who represents the customers, told Law360 in a Friday email that "BCBSA, as sponsors and administers of a health plan for federal employees, made certain promises regarding data security that they failed to live up to."

He added that they are hopeful BCBSA's attempt to escape responsibility will be as unsuccessful in this matter as it was in litigation over an Anthem Inc. data breach.

The 2015 breach, which affected 80 million people, is the subject of multidistrict litigation that, according to the customers in the present suit, BCBSA tried and failed to escape based on much of the same arguments it raises now.

Representatives for the other parties didn't immediately return request for comment Friday.

The customers are represented by Faraci Lange LLP, Weitz & Luxenberg PC,Faruqi & Faruqi LLP, Siprut PC, Ahdoot & Wolfson PC, Finkelstein Blankinship Frei-Pearson & Garber LLP, Chimicles & Tikellis LLP, Keller Rohrback LLP, Girard Gibbs LLP, Cohen & Malad LLP, Peiffer Rosca Wolf Abdullah Carr & Kane LLP and Robbins Geller Rudman & Dowd LLP, among others.

BCBSA is represented by Thomas S. D'Antonio, Brian P. Kavanaugh, Luke C. Ruse and Timothy C. Pickert of Kirkland & Ellis LLP and Adam P. Feinberg of Miller & Chevalier Chartered.

Excellus and Lifetime are represented by Paul Karlsgodt and David A. Carney of BakerHostetler and John G. Schmidt Jr., Jennifer A. Becakge and Mark J. Moretti of Phillips Lytle LLP.

The first case is Fero et al. v. Excellus Health Plan Inc. et al., case number 6:15-cv-06569, in the U.S. District Court for the Western District of New York.

— Additional reporting by Emily Field and Steven Trader. Editing by Ben Guilfoy.

All Content © 2003-2016, Portfolio Media, Inc.