

October 10, 2017

FTC's Unfairness Claim is Dismissed in Closely Watched Device Data Privacy-Based Action

The January 5, 2017, Complaint filed by the Federal Trade Commission ("FTC") in the U.S. District Court for the Northern District of California ("Court") against D-Link Corporation and D-Link Systems, Inc. (*Federal Trade Commission v. D-Link Corp.*, case number 3:17-cv-00039) is going to proceed beyond the initial pleading phase. On September 19, 2017, Judge James Donato issued his ruling to the Motion to Dismiss filed by D-Link Systems on January 31, 2017. While the order gives both parties standing to claim a victory, the substance of the order is an interesting roadmap to FTC privacy-related cases and it directly addressed the fact that the FTC failed to identify any actual consumer harm.

The case filed against D-Link Systems (D-Link Corporation was also sued, but was dismissed without prejudice via stipulation of the parties) represents an action against a company for allegedly leaving private consumer data vulnerable to hackers. However, as we previously reported, unlike other actions brought by the FTC, there is no evidence of a breach occurring or of any consumers suffering harm. The Court found that this was a sufficient failure to justify dismissal of three claims.

The complaint alleged that D-Link failed to take reasonable steps to secure its routers and internet protocol cameras despite promoting its products as "easy to secure" and having "advanced network security," or supporting "the latest wireless security features to help prevent unauthorized access, be it from a wireless network or from the Internet."

The Motion to Dismiss raised challenges pursuant to the Federal Rules of Civil Procedure Rules 8(a), 9(b) and 12(b)(6).

- The Rule 9(b) challenge had to do with whether the FTC's Complaint stated with particularity the circumstances constituting fraud or mistake. This analysis is interesting as the Complaint does not contain an express cause of action for fraud. However, Judge Donato interpreted the FTC's allegations regarding misleading the consumers to determine that the higher Rule 9(b) pleading standard must be met.
- Despite the FTC's argument that fraud is not an essential element of deception claim, the Court held that the Ninth Circuit had rejected that contention. (*Vess v. Ciba-Geigy Corp.*, USA 317 F.3d 1087, 1103-04 (9th Cir. 2003))
- The Court also analyzed whether the FTC's unfairness claim had to meet the higher pleading standard. Finding arguments on both sides of the issue, the Court made the determination to dismiss the claim as failing under even the lower pleading standard.
- The Court agreed with D-Link's argument that the FTC failed to allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Basically, the FTC alleges a "mere possibility of injury ..." (Order at pg. 8)
- The Court did provide the FTC with a roadmap suggesting that if the FTC tied its unfairness claim to the allegedly misleading data security representations, it would have a "more colorable injury element." (Order at pg. 9)

The Court did find that other than the unfairness claims, the remainder of the claims could survive the pleading challenge or at least be amended.

October 10, 2017

- The Court overruled the challenge to the second cause of action, which alleges that D-Link misrepresented the data security and protections its devices provide. While the Court acknowledged the challenge that the Complaint needed to allege specific consumer reliance, the Court found that at this stage, the FTC simply needed to allege particularized facts leading to a plausible inference of liability.
- The Court rejected D-Link's challenge that the unfairness claim as a whole was an overreach by the FTC. D-Link challenged the FTC's authority over data security practices. The Court flatly rejected this challenge. "Consequently, the fact that data security is not expressly enumerated as within the FTC's enforcement powers is of no moment to the exercise of its statutory authority." See also *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 259 (3d Cir. 2015) (finding that legislative acts affecting cybersecurity have not "reshaped the provision's [15 U.S.C. § 45(a)] meaning to exclude cybersecurity"). (Order pg. 6–7)
- The Court rejected D-Link's challenge to the lack of fair notice. "There can be no serious question that data security is a new and rapidly developing facet of our daily lives, and to require the FTC in all cases to adopt rules or standards before responding to data security issues faced by consumers is impractical and inconsistent with governing law." (Order pg. 7)

Ultimately, while the Court dismissed three counts, it did so with leave to amend. The FTC has until October 20, 2017, to file an amended pleading. While D-Link is rightly justified in claiming victory as some of the FTC's claims were knocked down, the FTC has the opportunity to amend. Whether and how the FTC chooses to amend the pleading will be very interesting. The Republican-led FTC has never been in favor of the case and it should be telling to see how aggressive an amended pleading will be or if one will even be filed.

There is no existing national law dictating how companies need to protect the data. The FTC, like the CFPB and other agencies, commonly "legislate" through enforcement actions or settlements. As very few companies elect to fight these actions, this will be an important case to follow.

Jonathan C. Sandler

Shareholder

jsandler@bhfs.com

310.564.8672

Richard B. Benenson

Shareholder

rbenenson@bhfs.com

303.223.1203

Evan M. Rothstein

Shareholder

erothstein@bhfs.com

303.223.1116

This document is intended to provide you with general information regarding Federal Trade Commission v. D-Link Corp. The contents of this document are not intended to provide specific legal advice. If you have any questions about the contents of this document or if you need legal advice as to an issue, please contact your regular Brownstein Hyatt Farber Schreck, LLP attorney. This communication may be considered advertising in some jurisdictions.