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

FTC Tests Limits Of Data Security Power In D-Link Action

By **Allison Grande**

Law360, New York (January 9, 2017, 4:35 PM EST) -- The Federal Trade Commission has dialed up its aggressive policing of corporate data security in faulting connected device manufacturer D-Link for missteps that allegedly left consumer data vulnerable but not exposed, but the company's decision to fight back and a looming change in leadership at the commission could spell the end for such security sweeps.

In a complaint filed in California federal court Thursday, the commission accused Taiwan-based computer networking equipment manufacturer D-Link Corp. of violating the unfairness and deception prongs of Section 5 of the FTC Act by leaving consumers' information vulnerable to hackers by allegedly failing to properly secure its wireless routers and internet protocol cameras and misleadingly touting its products as "easy to secure" or containing "advanced network security."

While the allegations of inadequate security and deceptive marketing promises come up often in FTC enforcement actions, particularly in the dozens of cases that the regulator has brought against companies for failing to maintain reasonable security practices, the D-Link action stands out because the FTC does not allege that any consumer data was actually exposed or that consumers have suffered any harm as a result of the company's purportedly shoddy security.

"This is a significant development in privacy and data security law," said Shook Hardy & Bacon LLP data security and privacy group co-chair Al Saikali. "Every single company needs to follow this enforcement action because if it is successful, then a security vulnerability alone in a consumer product — without actual access or acquisition of sensitive information — may be enough to trigger liability."

The FTC has not been shy about going after a broad range of companies in recent years for allegedly lax data security. In the internet of things space alone, the regulator within the past three years has hit hardware maker AsusTek Computer Inc. for alleged vulnerabilities in its routers and cloud services and security camera manufacturer Trendnet Inc. for security holes in its products that allowed hackers to webcast live feeds from hundreds of its customers' homes.

"There's no law right now that speaks to or dictates how companies need to protect and how to engage in their business with respect to the internet of things," Manatt Phelps & Phillips LLP partner and former FTC staff attorney Marc Roth said. "But nevertheless, the FTC, in the absence of such laws, has effectively been legislating by settlement, and the cases they bring and the advice they put out to companies lay out what the FTC expects companies to do to in order to protect customer information."

However, the D-Link case departs from the prior enforcement actions concerning connected device security in that the company refused to quickly settle the FTC's claims, which would have given at least some credence to the commission's unfairness and deception assertions. Instead, D-Link staunchly denied the allegations and said in a statement Thursday that it was taking steps to defend itself in the action.

"It's significant that D-Link is fighting back against the FTC, especially in light of the aggressive and preemptive approach that the commission is taking by bringing a case when there hasn't been a breach or an obvious injury that the FTC can hang its hat on," Fenwick & West LLP of counsel Hanley Chew said.

"It's definitely a possibility that the FTC might have some issues with the harm prong of the FTC Act, especially given the cases that commission typically brings and are successful in are instances where there has been a breach or some actual concrete harm or injury," he added.

If D-Link continues to press its challenge as anticipated, it would mark just the third time that a company has chosen to contest the agency's power to bring data security claims under the unfairness prong of Section 5.

One of the previous challenges, mounted by LabMD Inc., is still going strong after more than three years of litigation. The dispute is currently before the Eleventh Circuit, which has been asked to consider a July ruling in which the heads of the FTC overturned their own administrative law judge in concluding that the lab's failure to employ "basic" security precautions led to an unauthorized disclosure of sensitive medical data that caused "substantial" harm to consumers in violation of the unfairness prong.

The appellate court offered a glimpse into its take on the ruling in November, when it granted the lab's bid to stay enforcement of the order after concluding that the dispute presented substantial legal questions and that now-defunct LabMD would be irreparably harmed absent a stay.

"It's possible that the Eleventh Circuit decision suggesting that the harm standard may not be enough in the LabMD case may very well have bolstered D-Link to fight the FTC," Frankfurt Kurnit Klein & Selz PC partner Jeremy Goldman said. "The harm in the D-Link case seems even more speculative than in the LabMD case because at least in the LabMD case, there was a data file that was put out there that could have been misused."

D-Link's impending fight also shares similarities with the inaugural battle against the FTC's data security authority, which was mounted by Wyndham Worldwide Corp. In that dispute, the Third Circuit in August 2015 rejected the hotel chain's argument that the commission didn't have the power to categorize a failure to institute reasonable data security practices as "unfair" and had failed to give businesses reasonable notice of how it planned to wield its authority. That dispute ended less than four months after the appellate court's ruling, when the sides agreed to a settlement.

However, attorneys were quick to note that in the Wyndham dispute, the FTC was able to point to three separate payment card breaches that exposed more than 600,000 consumer payment card account numbers and led to more than $10.6 million in fraud loss to prop up its unfairness claim, which is not the case with the D-Link complaint.

"In other words, the FTC is doubling down [with the D-Link complaint]," Saikali said. "It’s saying not only is a breach enough, without demonstrable injury as in LabMD and Wyndham, but a vulnerability that

might later lead to a cyberattack that might then later lead to demonstrable injury is enough. It's stacking inference on inference, which is dangerous and opens a whole new can of worms for companies."

Therefore, the outcome of both of the two pending matters will be crucial for companies to watch, attorneys noted.

"The D-Link case is an example of the FTC's ongoing approach to make privacy policy through targeted enforcement actions, in this case in the connected device environment where personal information, including intimate details about daily life, can be shared and misappropriated," Goodwin Procter LLP partner Karen Neuman said. "As the Internet of Things matures, the various service providers will have to understand the underlying relationships, along with their responsibility for protecting privacy and securing data. The FTC will continue to exert its authority and provide guidance in this area by issuing best practices and bringing enforcement actions, so it will be interesting to see how this plays out."

The cases are also worth keeping an eye on due to the potential for a circuit split. Julie Brill, who served as an FTC commissioner until last April, when she stepped down and became co-director of Hogan Lovells' global privacy and cybersecurity practice, noted that she found it interesting that the two commissioners who voted to bring the complaint — Republican Commissioner Maureen Ohlhausen voted against the filing — elected to lodge the suit in California federal court instead of initiate an administrative complaint as the agency had against LabMD.

"The FTC may have decided to proceed in federal court to place itself in the strongest position in any potential appeal," Brill said. "Rather than allowing the defendant to control which circuit court would hear the appeal — and risk the potential that the defendant files its appeal in the Eleventh Circuit, which is currently hearing the LabMD appeal — the agency has determined that it would like the Ninth Circuit to hear any potential appeal."

Combined with Ohlhausen's vote against bringing the action, "the forum choice may demonstrate that the facts and law at issue in this case are closer to the edge of practices that previously have been found to be unfair under Section 5 than might be apparent from the FTC's complaint," Brill added.

The Republican commissioner's dissent could also foreshadow what is to come at the commission under the administration of President-elect Donald Trump, attorneys noted.

Currently, the commission comprises a Republican and two Democrats, including Chairwoman Edith Ramirez. The chair and fellow Democrat Terrell McSweeney voted in favor of bringing the action against D-Link while Ohlhausen — who is a front-runner to assume the chair position and has often pushed back at the commission's efforts to expand its authority beyond concrete harms — dissented without providing her reasoning.

"It's very likely that there will be a definite slowing down in these cases with the new administration," Roth said. "Especially if Commissioner Ohlhausen gets the nod to lead the commission or someone with similar sensibilities is put in there, I don't see these cases being brought without proof of actual harm."

However, Brill cautioned that observers shouldn't be too quick to prejudge the outcome of the D-Link or LabMD disputes or what Ohlhausen and other Republicans may do in future cases.

"There's probably more than meets the eye to this matter," Brill said. "We certainly know that Commissioner Ohlhausen has a more exacting standard for harm under the unfairness test ... but there could have been number of things that caused her to dissent. And while the agency is attempting to position its case as falling right within the contours of other cases that it has brought, at this point in time, we're only seeing one side of the story."

But regardless of how the disputes end up, attorneys agree that the most egregious data security violations will continue to catch the eye of the regulator, especially in the wake of hackers hijacking millions of internet-connected devices to help them carry out a major cyberattack on domain name service provider Dyn Inc. in October that temporarily blocked access to popular websites such as Twitter and The New York Times.

Therefore, companies need to be sure to take steps to put in basic security precautions to safeguard the sensitive data they hold, attorneys say.

"Routers and this kind of camera aren't exactly new, but the FTC is highlighting fairly straightforward weaknesses in these devices," Wiley Rein LLP privacy practice chair Kirk Nahra said. "[This complaint] is an important reminder to both consumers and companies to make sure that the easy stuff is being done correctly."

The FTC is represented by staff attorneys Laura D. Berger, Kevin H. Moriarty and Cathlin Tully.

Counsel information for D-Link was not immediately available.

The case is Federal Trade Commission v. D-Link Corp. et al., case number 3:17-cv-00039, in the U.S. District Court for the Northern District of California.

--Editing by Christine Chun and Katherine Rautenberg.
