FTC Files Lawsuit Against Taiwanese Manufacturer for Alleged Lax Security in Wireless Routers and Cameras and Related Marketing Claims

Dana B. Rosenfeld, Alysa Z. Hutnik

January 6, 2017

The Federal Trade Commission has filed a lawsuit in federal court claiming that a networking equipment manufacturer engaged in unfair and deceptive acts, exposing thousands of consumers to the risk of cyberattack from vulnerable wireless routers and internet cameras.

The complaint against Taiwan-based networking equipment manufacturer D-Link Corporation and its U.S. subsidiary D-Link Systems alleges that the companies failed to take reasonable steps to protect the internet routers and IP cameras from "widely known and reasonable foreseeable" vulnerabilities. According to the complaint, these risks were not purely theoretical: D-Link equipment has been compromised by attackers, including being made part of "botnets," which are large-scale networks of computers infected by malicious software.

In particular, the complaint alleges that the company failed to take steps to address well-known and easily preventable security flaws, such as:

- "hard-coded" login credentials integrated into D-Link camera software -- such as the username "guest" and the password "guest" -- that could allow unauthorized access to the cameras' live feed;
- a software flaw known as "command injection" that could enable remote attackers to take control of consumers' routers by sending them unauthorized commands over the Internet;
- the mishandling of a private key code used to sign into D-Link software, such that it was openly available on a public website for six months; and
- leaving users' login credentials for D-Link's mobile app unsecured in clear, readable text on their mobile devices, even though there is free software available to secure the information.

Count I of the complaint alleges that D-Link's failure to take reasonable measures to secure the products from these vulnerabilities was **unfair** under Section 5 of the FTC act. It alleges that D-Link's practices caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

But the FTC is not only concerned with the potential vulnerabilities of the D-Link products; in Counts II through VI, the FTC alleges that D-Link violated Section 5(a) of the FTC Act by making **deceptive**

statements about the products' security. These allegedly deceptive statements include the following:

Count II: D-Link advertised a Security Event Response Policy, implying that D-Link had taken reasonable measures to secure the products from unauthorized access;

Count III: In promotional materials, D-Link claimed that its routers were "EASY TO SECURE" and had "ADVANCED NETWORK SECURITY," among other claims, implying that the routers were secure from unauthorized access and control;

Count IV: In promotional materials, D-Link advertised that its cameras provided a "secure connection," among other claims, implying that the cameras were secure from unauthorized access and control;

Count V: To begin using the routers, a graphical user interface provided security-related prompts such as "To secure your new networking device, please set and verify a password below," implying that the routers were secure from unauthorized access and control; and

Count VI: To begin using the cameras, a graphical user interface provided security-related prompts such as "Set up an Admin ID and Password" or "enter a password" in order "to secure your camera" and featured a lock logo, implying that the cameras were secure from unauthorized access and control.

In a press release announcing the lawsuit, FTC Bureau of Consumer Protection Director Jessica Rich commented, "When manufacturers tell consumers that their equipment is secure, it's critical that they take the necessary steps to make sure that's true."

The Commission vote authorizing the staff to file the complaint was 2-1, with Commissioner Maureen K. Ohlhausen voting against the complaint. The complaint was filed in the U.S. District Court for the Northern District of California.

The complaint is just the most recent action in the FTC's efforts to crack down on potential vulnerabilities in the Internet of Things (IoT). The FTC has also brought enforcement actions against ASUS over allegedly insecure routers and cloud services and against TRENDnet over its allegedly insecure cameras. This case serves as yet another reminder that the FTC remains focused on cyber security, especially for IoT devices, and that it is important for all businesses that handle or have access to customer information to ensure that they have implemented reasonable security practices, and confirmed the accuracy of all related marketing claims and public representations (including in public-facing policies and product dashboards) about the security of their products.