DAVID SHONKA
Acting General Counsel

LAURA D. BERGER (FL Bar No. 11762)
Federal Trade Commission
901 Market Street, Suite 570
San Francisco, CA 94103
P: (202) 326-2471/F: (415) 848-5184
lberger@ftc.gov;

KEVIN H. MORIARTY (DC Bar No. 975904)
CATHLIN TULLY (NY Bar)
Federal Trade Commission
600 Pennsylvania Ave N.W.
Washington, DC 20580
P: (202) 326-3644/F: (202) 326-3062
kmoriarty@ftc.gov; ctully@ftc.gov

Attorneys for Plaintiff Federal Trade Commission

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FEDERAL TRADE COMMISSION, Plaintiff, v. D-LINK CORPORATION and D-LINK SYSTEMS, INC., corporations, Defendants.	No. 3:17-CV-00039-JD **COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF**

1. Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint, brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C.

§ 53(b), to obtain permanent injunctive relief and other equitable relief against Defendants for engaging in unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendants' failure to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

3. Venue in the Northern District of California is proper under 28 U.S.C. § 1391(b) and (c) and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and to secure such other equitable relief as may be appropriate in each case. 15 U.S.C. §§ 53(b), 56(a)(2)(A).

DEFENDANTS

6. Defendant D-Link Corporation ("D-Link") is a Taiwanese corporation with its principal office or place of business at No. 289, Xinhu 3rd Rd., Neihu District, Taipei City, Taiwan 114. D-Link transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, D-Link purposefully directed its activities to the United States by designing, developing, marketing, and manufacturing routers, Internet-protocol ("IP") cameras, and related software and services, intended for use by consumers throughout the United States.

7. Defendant D-Link Systems, Inc., ("DLS") is a California corporation with its principal office or place of business at 17595 Mt. Herrmann St., Fountain Valley, California

92708. DLS transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, DLS has advertised, marketed, distributed, or sold routers, IP cameras, and related software and services, intended for use by consumers throughout the United States. The Chairman of DLS's Board of Directors has served as D-Link's Chief Executive Officer and the two entities have coordinated closely regarding the security of Defendants' routers and IP cameras.

8. The FTC's claims against D-Link and DLS arise from or relate to Defendants' acts or practices aimed at or taking place in the United States.

COMMERCE

9. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS PRACTICES

10. D-Link is a hardware device manufacturer that designs, develops, markets, and manufactures networking devices, including devices with core functions that relate to security, such as consumer routers and IP cameras. D-Link designs, develops, and manufactures these products, their marketing materials, and related software and services for distribution or sale to United States consumers through its subsidiary, DLS. D-Link is responsible for providing ongoing support to DLS for its products, including by remediating any design, usability, and security issues in Defendants' routers and IP cameras. D-Link also conducts security testing of the software for Defendants' routers and IP cameras. When releasing new software for such routers and IP cameras, D-Link uses a digital signature issued in its name, known as a "private key," to sign the software, in order to assure entities, such as browsers and operating systems, that the software comes from an authentic or "trusted" source and is not malware.

11. DLS is a subsidiary of D-Link and is nearly 98% owned by D-Link and its holding company, D-Link Holding Company, Ltd. DLS provides marketing and after-sale services integral to D-Link's operations, including by marketing and acting as the sole

distributor of Defendants' routers and IP cameras throughout the United States. DLS also recommends to D-Link features that D-Link should include in products designed for the United States market. Among other services, DLS acts as the primary point-of-contact for problems that United States consumers have with Defendants' routers, IP cameras, or related software and services; conducts initial inquiries into the validity of security vulnerability reports for products sold in the United States; and transmits to D-Link any such reports that it believes may warrant software security updates from D-Link. DLS also assists in notifying United States consumers about the availability of security updates through means such as DLS's websites.

12. Defendants have provided software applications that enable users to access their routers and IP cameras from a mobile device ("mobile apps"), including a free "mydlink Lite" mobile app. Defendants designed the mydlink Lite app to require the user to enter a user name and password ("login credentials") the first occasion that a user employs the app on a particular mobile device. After that first occasion, the app stores the user's login credentials on that mobile device, keeping the user logged into the mobile app on that device.

DEFENDANTS' ROUTERS

13. Defendants' routers, like other routers, operate to forward data packets along a network. In addition to routing network traffic, they typically play a key role in securing consumers' home networks, functioning as a hardware firewall for the local network, and acting as the first line of defense in protecting consumer devices on the local network, such as computers, smartphones, IP cameras, and other connected appliances, against malicious incoming traffic from the Internet.

DEFENDANTS' IP CAMERAS

14. Defendants' IP cameras, akin to many such IP cameras, play a key security role for consumers, by enabling consumers to monitor private areas of their homes or businesses, to detect any events that may place the property or its occupants at risk. In many instances, Defendants offer them as a means to monitor the security of a home while consumers are away,

or to monitor activities within the household, including the activities of young children, while a consumer is at home. Consumers seeking to monitor the security of their homes or the safety of young children may access live video and audio feeds ("live feeds") from their cameras over the Internet, using a mobile device or other computer.

DEFENDANTS' SECURITY FAILURES

15. Defendants have failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access, including by failing to protect against flaws which the Open Web Application Security Project has ranked among the most critical and widespread web application vulnerabilities since at least 2007. Among other things:

a. Defendants repeatedly have failed to take reasonable software testing and remediation measures to protect their routers and IP cameras against well-known and easily preventable software security flaws, such as "hard-coded" user credentials and other backdoors, and command injection flaws, which would allow remote attackers to gain control of consumers' devices;

b. Defendant D-Link has failed to take reasonable steps to maintain the confidentiality of the private key that Defendant D-Link used to sign Defendants' software, including by failing to adequately restrict, monitor, and oversee handling of the key, resulting in the exposure of the private key on a public website for approximately six months; and

c. Defendants have failed to use free software, available since at least 2008, to secure users' mobile app login credentials, and instead have stored those credentials in clear, readable text on a user's mobile device.

THOUSANDS OF CONSUMERS AT RISK

16. As a result of Defendants' failures, thousands of Defendants' routers and cameras have been vulnerable to attacks that subject consumers' sensitive personal information and local networks to a significant risk of unauthorized access. In fact, the press

has reported that Defendants' routers and cameras have been vulnerable to a range of such attacks and have been compromised by attackers, including by being made part of large scale networks of computers infected by malicious software, known as "botnets."

17. The risk that attackers would exploit these vulnerabilities to harm consumers was significant. In many instances, remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable. For example, remote attackers could search for vulnerable devices over the Internet and obtain their IP addresses using readily available tools, such as a popular search engine that can locate devices running particular software versions or operating in particular locations. Alternatively, attackers could use readily accessible scanning tools to identify vulnerable devices operating in particular areas or on particular networks. In many instances, an attacker could then take simple steps to exploit vulnerabilities in Defendants' routers and IP cameras, impacting not only consumers who purchased these devices, but also other consumers, who access the Internet in public or private locations served by the routers or who visit locations under the IP cameras' surveillance.

18. By creating these vulnerabilities, Defendants put consumers at significant risk of harm in a variety of ways. An attacker could compromise a consumer's router, thereby obtaining unauthorized access to consumers' sensitive personal information. For example, using a compromised router, an attacker could re-direct consumers seeking a legitimate financial site to a spoofed website, where they would unwittingly provide the attacker with sensitive financial account information. Alternatively, using a compromised router, an attacker could obtain consumers' tax returns or other files stored on the router's attached storage device or could use the router to attack other devices on the local network, such as computers, smartphones, IP cameras, or connected appliances. Similarly, by exploiting the vulnerabilities described in Paragraph 15, an attacker could compromise a consumer's IP camera, thereby monitoring consumers' whereabouts to target them for theft or other criminal activity or to observe and record over the Internet their personal activities and conversations or those of their young children. In many instances, attackers could carry out such exploits covertly, such that

consumers would have no reason to know that an attack was ongoing. Finally, during the time Defendant D-Link's private key was available on a public website, consumers seeking to download legitimate software from Defendants were at significant risk of downloading malware, signed by malicious actors using D-Link's private key.

DEFENDANTS' SECURITY STATEMENTS

19. Defendants have disseminated or caused to be disseminated to consumers statements regarding the security of their products, including their routers and IP cameras.

SECURITY EVENT RESPONSE POLICY

20. From approximately December 2013 until early September 2015, after highly-publicized security flaws were found to affect many of its products, Defendant DLS posted a Security Event Response Policy on its product support webpage, **http://support.dlink.com/securityadvisories.aspx**, in the general form of Exhibit 1. Within its Security Event Response Policy, under a bolded heading "D-Link's commitment to Product Security," Defendant DLS stated:

> D-Link prohibits at all times, including during product development by D-Link or its affiliates, any intentional product features or behaviors which allow unauthorized access to the device or network, including but not limited to undocumented account credentials, covert communication channels, 'backdoors' or undocumented traffic diversion. All such features and behaviors are considered serious and will be given the highest priority.

PROMOTIONAL CLAIMS

21. Defendants highlight their routers' security features in a wide range of materials available on Defendant DLS's website, including user manuals and promotional brochures, which describe these features alongside language that specifically references the device's "security". Such materials include, but are not limited to, brochures in the general form of Exhibits 2-5, which state:

a. Under a bolded, italicized, all-capitalized heading, "***EASY TO SECURE***," that the router:

> supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption, regardless of your client devices. In addition [the router] utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.
>
> Delivering great wireless performance, network security and coverage [the router] is ideal for upgrading your existing wireless network. (*See* PX 2).

b. Under a bolded, italicized, all-capitalized heading, "***ADVANCED NETWORK SECURITY***," that the router:

> ensures a secure Wi-Fi network through the use of WPA/WPA2 wireless encryption. Simply press the WPS button to quickly establish a secure connection to new devices. The [router] also utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks and intrusions from across the Internet. (*See* PX 3).

c. Under a bolded heading, "**Advanced Network Security**," that the router:

> supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption method. In addition, this [router] utilizes Stateful Packet Inspection Firewalls (SPI) to help prevent potential attacks from across the Internet. (*See* PX 4).

d. Under a heading "128-bit Security Encryption," that the router:

> protects your network with 128-bit AES data security encryption – the same technology used in E-commerce or online banking. Create your own network

> name and password or put it at the tip of your fingers with 'Push Button Security' standard on every Amplifi device. With hassle-free plug and play installation, and advanced Wi-Fi protected setup, the [router] is not only one of the fastest routers available, its [sic] also one of the safest. (*See* PX 5).

22. Defendants highlight the security of their IP cameras in a wide range of materials available on Defendant DLS's website, including user manuals and promotional brochures, which describe these features alongside language that specifically references the device's "security". Such materials include, but are not limited to, brochures in the general form of Exhibit 6, which display the word "SECURITY" in large, capital letters, in a vividly-colored footer across the bottom of each page. (*See* PX 6). In addition, Defendants have designed their IP camera packaging, including in the general form of Exhibit 7, to display security-related terms. Such terms include the words "secure connection," next to a lock icon, among the product features listed on the side of the box (*see* PX 7).

INTERACTIVE SECURITY FEATURES

23. Defendants' routers offer numerous security features that Defendants present alongside instructions that specifically reference the device's "security". In particular, in many instances, to begin using the router, users must access a graphical user interface (hereinafter, "Defendants' router GUI"), in the general form of Exhibits 8 and 9, which includes instructions, such as:

a. "To secure your new networking device, please set and verify a password below" (*see* PX 8); and

b. "It is highly recommended that you create a password to keep your router secure." (*See* PX 9).

24. Defendants' IP cameras offer numerous security features that Defendants present alongside language that specifically references the device's "security". In particular, to begin using the camera, in many instances, users must access a GUI (hereinafter "Defendants' IP camera GUI"), in the general form of Exhibits 10 and 11, which include language, such as:

a. instructions to "Set up an Admin ID and Password" or "enter a password" in order "to secure your camera" (*see* PX 10); and

b. security-related banners, including, but not limited to, the words "SECURICAM Network," alongside a lock icon, across the top of the GUI (*see* PX 11).

D-LINK DIRECTS ITS PRACTICES TO U.S. CONSUMERS

25. D-Link controls decisions about which products and features Defendants will offer to United States consumers. Upon deciding to design and develop a new product for sale in the United States, D-Link is responsible for writing the "Product Requirements Document," which sets forth the functions and features that the product will possess, including any security features. D-Link also controls decisions about whether to conduct security testing and review of these products and their related software, before offering them to U.S. consumers. Further, to the extent that D-Link decides to conduct security review and testing of a product before offering it to United States consumers, D-Link is responsible for conducting or procuring such review and testing and for determining whether the results warrant revisions to the product. Once a new product is launched in the United States, D-Link is responsible for providing ongoing support to DLS for the product, including by determining whether to remediate any design, usability, and security issues that are reported in Defendants' routers and IP cameras. For example, if a security vulnerability is reported in Defendants' routers or IP cameras and related software, D-Link is responsible for determining whether a security update is warranted to address the vulnerability and, if so, for developing the update. When D-Link develops new products for United States consumers, DLS may request that D-Link include certain features in the products, but DLS does not participate in drafting the Product Requirements Documents or in designing and testing any security features these products may have.

VIOLATIONS OF THE FTC ACT

26. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

27. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

Unfairness

28. In numerous instances, Defendants have failed to take reasonable steps to secure the software for their routers and IP cameras, which Defendants offered to consumers, respectively, for the purpose of protecting their local networks and accessing sensitive personal information.

29. Defendants' practices caused, or are likely to cause, substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

30. Therefore, Defendants' acts and practices as described in Paragraphs 15-18 of this Complaint constitute unfair acts or practices in or affecting commerce, in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

COUNT II

Security Event Response Policy Misrepresentation

31. Through the means described in Paragraph 20, Defendant DLS has represented, directly or indirectly, expressly or by implication, that Defendants took reasonable steps to secure their products from unauthorized access.

32. In truth and in fact, as described in Paragraphs 15-18, Defendants did not take reasonable steps to secure their products from unauthorized access.

33. Therefore, the making of the representation set forth in Paragraph 31 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

Router Promotional Misrepresentations

34. Through the means described in Paragraph 21, Defendants have represented, directly or indirectly, expressly or by implication, that the routers described by these claims were secure from unauthorized access.

35. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were not secure from unauthorized access and control.

36. Therefore, the making of the representation set forth in Paragraph 34 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT IV

IP Camera Promotional Misrepresentations

37. Through the means described in Paragraph 22, Defendants have represented, directly or indirectly, expressly or by implication, that the IP cameras described by these claims were secure from unauthorized access and control.

38. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras were not secure from unauthorized access and control.

39. Therefore, the making of the representation set forth in Paragraph 37 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT V

Router GUI Misrepresentations

40. Through the means described in Paragraph 23, Defendants have represented, directly or indirectly, expressly or by implication, that the routers described by these claims were secure from unauthorized access.

41. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were not secure from unauthorized access and control.

42. Therefore, the making of the representation set forth in Paragraph 40 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT VI

IP Camera GUI Misrepresentations

43. Through the means described in Paragraph 24, Defendants have represented, directly or indirectly, expressly or by implication, that the IP cameras described by these claims were secure from unauthorized access and control.

44. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras were not secure from unauthorized access and control.

45. Therefore, the making of the representation set forth in Paragraph 43 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

46. Consumers are likely to suffer substantial injury as a result of Defendants' violations of the FTC Act. Absent injunctive relief by this Court, Defendants are likely to injure consumers and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

47. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendants; and

B. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

DAVID SHONKA
Acting General Counsel

Dated: January 5, 2017

/s/ Cathlin Tully
LAURA D. BERGER
KEVIN H. MORIARTY
CATHLIN TULLY

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION