

1 DAVID SHONKA
Acting General Counsel

2
3 LAURA D. BERGER (FL Bar No. 11762)
Federal Trade Commission
4 901 Market Street, Suite 570
San Francisco, CA 94103
5 P: (202) 326-2471/F: (415) 848-5184
6 lberger@ftc.gov;

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

11
12 *Attorneys for Plaintiff Federal Trade Commission*

13 **UNITED STATES DISTRICT COURT**
14 **NORTHERN DISTRICT OF CALIFORNIA**
15 **SAN FRANCISCO DIVISION**

16 FEDERAL TRADE COMMISSION,)
17)
18 Plaintiff,)
19 v.)
20 D-LINK CORPORATION)
21 and)
22 D-LINK SYSTEMS, INC.,)
corporations,)
23 Defendants.)
24)

Case No. _____

**COMPLAINT FOR
PERMANENT INJUNCTION AND
OTHER EQUITABLE RELIEF**

25
26 1. Plaintiff, the Federal Trade Commission (“FTC”), for its Complaint, brings this
27 action under Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C.

1 § 53(b), to obtain permanent injunctive relief and other equitable relief against Defendants for
2 engaging in unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15
3 U.S.C. § 45(a), in connection with Defendants' failure to take reasonable steps to secure the
4 routers and Internet-protocol cameras they designed for, marketed, and sold to United States
5 consumers.

6 **JURISDICTION AND VENUE**

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

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

11 **PLAINTIFF**

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

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

18 **DEFENDANTS**

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

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

1 92708. DLS transacts or has transacted business in this district and throughout the United States.
2 At all times material to this Complaint, acting alone or in concert with others, DLS has
3 advertised, marketed, distributed, or sold routers, IP cameras, and related software and services,
4 intended for use by consumers throughout the United States. The Chairman of DLS's Board of
5 Directors has served as D-Link's Chief Executive Officer and the two entities have coordinated
6 closely regarding the security of Defendants' routers and IP cameras.

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

9 **COMMERCE**

10 9. At all times material to this Complaint, Defendants have maintained a substantial
11 course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act,
12 15 U.S.C. § 44.

13 **DEFENDANTS' BUSINESS PRACTICES**

14 10. D-Link is a hardware device manufacturer that designs, develops, markets, and
15 manufactures networking devices, including devices with core functions that relate to security,
16 such as consumer routers and IP cameras. D-Link designs, develops, and manufactures these
17 products, their marketing materials, and related software and services for distribution or sale to
18 United States consumers through its subsidiary, DLS. [REDACTED]

19 [REDACTED]
20 [REDACTED]
21 [REDACTED] When releasing new software for such
22 routers and IP cameras, D-Link uses a digital signature issued in its name, known as a "private
23 key," to sign the software, in order to assure entities, such as browsers and operating systems,
24 that the software comes from an authentic or "trusted" source and is not malware.

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

1 distributor of Defendants’ routers and IP cameras throughout the United States. [REDACTED]

2 [REDACTED]
3 [REDACTED] Among other services, DLS acts as the primary point-of-contact for
4 problems that United States consumers have with Defendants’ routers, IP cameras, or related
5 software and services; [REDACTED]

6 [REDACTED]
7 [REDACTED] DLS also assists in notifying
8 United States consumers about the availability of security updates through means such as
9 DLS’s websites.

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

16 **DEFENDANTS’ ROUTERS**

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

23 **DEFENDANTS’ IP CAMERAS**

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

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

5 **DEFENDANTS’ SECURITY FAILURES**

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

10 Among other things:

- 11 a. Defendants repeatedly have failed to take reasonable software testing and
12 remediation measures to protect their routers and IP cameras against well-
13 known and easily preventable software security flaws, such as “hard-coded”
14 user credentials and other backdoors, and command injection flaws, which
15 would allow remote attackers to gain control of consumers’ devices;
- 16 b. Defendant D-Link has failed to take reasonable steps to maintain the
17 confidentiality of the private key that Defendant D-Link used to sign
18 Defendants’ software, including by failing to adequately restrict, monitor, and
19 oversee handling of the key, resulting in the exposure of the private key on a
20 public website for approximately six months; and
- 21 c. Defendants have failed to use free software, available since at least 2008, to
22 secure users’ mobile app login credentials, and instead have stored those
23 credentials in clear, readable text on a user’s mobile device.

24 **THOUSANDS OF CONSUMERS AT RISK**

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

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

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

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

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

5 **DEFENDANTS' SECURITY STATEMENTS**

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

8 **SECURITY EVENT RESPONSE POLICY**

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

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

21 **PROMOTIONAL CLAIMS**

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

1 a. Under a bolded, italicized, all-capitalized heading, “***EASY TO SECURE***,” that
2 the router:

3 supports the latest wireless security features to help prevent unauthorized
4 access, be it from over a wireless network or from the Internet. Support for
5 WPA™ and WPA2™ standards ensure that you will be able to use the best
6 possible encryption, regardless of your client devices. In addition [the router]
7 utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from
8 across the Internet.

9 Delivering great wireless performance, network security and coverage [the
10 router] is ideal for upgrading your existing wireless network. (See PX 2).

11 b. Under a bolded, italicized, all-capitalized heading, “***ADVANCED NETWORK
12 SECURITY***,” that the router:

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

18 c. Under a bolded heading, “**Advanced Network Security**,” that the router:

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

25 d. Under a heading “128-bit Security Encryption,” that the router:

26 protects your network with 128-bit AES data security encryption – the same
27 technology used in E-commerce or online banking. Create your own network
28

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

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

14 **INTERACTIVE SECURITY FEATURES**

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

- 20 a. “To secure your new networking device, please set and verify a password
21 below” (see PX 8); and
22 b. “It is highly recommended that you create a password to keep your router
23 secure.” (See PX 9).

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

1 **Router Promotional Misrepresentations**

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

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

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

10 **COUNT IV**

11 **IP Camera Promotional Misrepresentations**

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

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

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

20 **COUNT V**

21 **Router GUI Misrepresentations**

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

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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