Filing # 258584264 E-Filed 10/06/2026 11:41:18 AM

IN THE CIRCUIT COURT OF THE TENTH JUDICIAL CIRCUIT

POLK COUNTY, FLORIDA

OFFICE OF THE ATTORNEY GENERAL, STATE OF FLORIDA, DEPARTMENT OF LEGAL AFFAIRS, Plaintiff, v. TP-LINK SYSTEMS INC., Defendant.	Case No. _____

COMPLAINT

1. A router serves as a consumer's virtual mouth and ears to the internet. What the consumer says to the internet comes out of the router's mouth, and what the internet says back goes through the router's ears. If compromised, it can whisper lies in both directions, impersonating the consumer and creating a foothold in the consumer's own home for state-sponsored cyberattacks. As the Federal Communications Commission ("FCC") has explained, "[c]ompromised routers can enable in-depth network surveillance, data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses' networks."[1]

[1] FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List, WC Docket No. 18-89,

2. Such activity not only puts a consumer's internet connection at risk but also makes consumers involuntary participants in malicious campaigns carried out on behalf of foreign nations, something no Floridian would consent to. This is not hypothetical for the Florida Consumers who bought Defendant TP-Link Systems Inc. ("TP-Link" or "Defendant") routers that were subject to the Volt and Flax Typhoon attacks by Chinese state-sponsored hackers[2] or that were used by Chinese threat actor "Storm-0940" in password-spray attacks.[3]

3. Home- and small-office routers are typically housed within a consumer's own home or business and use the consumer's assigned IP address. According to TP-Link's website, a router connects devices, such as computers, phones, smart home devices, and security cameras, to the internet and manages the flow of data between them. Routers assign IP addresses for each device, manage bandwidth, and act as a basic security firewall between devices and the internet.[4] Given the sensitive

---

Public Notice, DA 26-278, App. C at 1 (Mar. 23, 2026) ("Routers Public Notice"), https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf.

[2] *See, e.g.*, End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, 119th Cong. (March 5, 2025) (statement of Rob Joyce), https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf.

[3] Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network, Microsoft (October 31, 2024), https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/.

[4] TP-Link, What Is a Router and Which One is Right For You? Everything You Need to Know, https://www.tp-link.com/us/blog/2499/what-is-a-router-and-which-one-is-right-for-you-everything-you-need-to-know/ (last visited Oct. 6, 2026), archived at https://perma.cc/4H2M-ZB7J.

information that consumers send and receive over the internet via their routers, it is imperative that companies that manufacture and market routers speak truthfully about their devices' functions and security risks.

4. TP-Link has amassed a large market share of the routers that consumers and small businesses purchase at retail. According to congressional testimony, TP-Link controls at least 60 percent of the United States retail market for Wi-Fi systems and small-office/home-office routers.[5]

5. Recognizing the importance of security to its consumers, TP-Link repeatedly represents that its routers have robust protections and features. For example, TP-Link tells consumers that its built-in "HomeShield" service "covers all security scenarios"; "handles all your concerns" regarding "private info leakage," "cyber virus intrusion," and "IoT device attacks"; and allows the user to "[c]heck the results of the scans and preventions against any potential cyber threats or attacks for your home network."[6] A version of TP-Link's website available as recently as

---

[5] End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses Before the H. Select Comm. on the Strategic Competition Between the U.S. and the Chinese Communist Party, 119th Cong. (Mar. 5, 2025) (statement of Rob Joyce, former Dir. of Cybersecurity, Nat'l Sec. Agency), https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf ("TP-Link, the world's largest manufacturer of commercial Wi-Fi and home routers has grown to at least 60% of the U.S. retail market for Wi-Fi systems and SoHo routers compared with about 10% of the market at the start of 2019.").

[6] TP-Link, HomeShield, https://www.tp-link.com/us/homeshield/ (last visited Oct. 6, 2026), archived at https://perma.cc/M8ME-4EX7.

November 2025 represented that HomeShield provides a "100% safeguard" for network security.[7]

6. TP-Link also makes model-specific security representations about its routers. TP-Link advertised its TL-WR940N router as providing "[e]asy wireless security encryption at a push of [a] WPS button," its Archer C7 as "provid[ing] secure Wi-Fi access for guests," and its Archer AX21 as offering "Refined Password Security" and a "New Level of Cyber Security."[8]

7. TP-Link's representations to Florida consumers and actions described here constitute "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce" under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Florida Stat. § 501.204(1).

8. *First*, TP-Link minimizes the risks to consumers from its longstanding and ongoing connections to China. By its own admission, TP-Link was not a separate company from its Chinese operations until 2024. China has been designated a foreign

---

[7] TP-Link, HomeShield (archived Nov. 14, 2025), https://web.archive.org/web/20251114185316/https://www.tp-link.com/us/homeshield/.

[8] TP-Link, TL-WR940N Product Page (archived Mar. 29, 2023), https://web.archive.org/web/20230329192916/https://www.tp-link.com/us/home-networking/wifi-router/tl-wr940n/; TP-Link, Archer C7 Product Page (archived Mar. 31, 2026), https://web.archive.org/web/20260331134655/https://www.tp-link.com/us/home-networking/wifi-router/archer-c7/; TP-Link, Archer AX21 Product Page (archived Oct. 6, 2022), https://web.archive.org/web/20221006205422/https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/.

adversary by the U.S. government.[9] Under China's 2017 National Intelligence Law, Chinese companies and citizens are required to "support, assist, and cooperate with national intelligence efforts in accordance with law" and to "protect national intelligence work secrets they are aware of."[10] Under China's 2021 Regulations on the Management of Security Vulnerabilities in Network Products ("RMSV"), Chinese tech providers and network operators must report (within 2 days) any newly discovered ("zero-day") security vulnerabilities.[11] A senior U.S. Department of Homeland Security ("DHS") official has reported that China appears to use the RMSV to preview zero-day flaws before companies can develop fixes.[12]

---

[9] 15 C.F.R. § 791.4.

[10] PRC National Intelligence Law art. 7 (as amended 2018), China Law Translate (June 27, 2017), https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/. The Chinese-language original has been rendered in varying English translations; *compare id.*, with https://cs.brown.edu/courses/cs180/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf.

[11] Stewart Scott et al., *Dragon Tails: Preserving International Cybersecurity Research*, Atlantic Council (Sept. 2022), https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/; *see also* Suzanne Smalley, *China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says*, CyberScoop (Aug. 10, 2022), https://cyberscoop.com/dhs-official-chinese-rules-exploit/ (reporting remarks of DHS Under Secretary for Policy Robert Silvers).

[12] Stewart Scott *et al.*, Dragon Tails: Preserving International Cybersecurity Research, Atlantic Council (Sept. 2022), https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/; Suzanne Smalley, China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says, CyberScoop (Aug. 10, 2022), https://cyberscoop.com/dhs-official-chinese-rules-exploit/ (reporting remarks of DHS Under Secretary for Policy Robert Silvers).

9. By TP-Link's own admission, it was affiliated with a Chinese company until 2024, when it finalized its separation from TP-Link Technologies Co., Ltd. ("TP-Link Technologies").

10. Even following its claimed split in mid-2024, TP-Link still makes misleading statements about its ties to China. TP-Link represents that "[a]s a company headquartered in the United States, no government—foreign or domestic—has access to and control over the design and production of our routers and other devices." [13] But much of TP-Link's research, development, and manufacturing remains in China, entrenched in China's state-sponsored technology ecosystem, with the company's leadership acknowledging accolades and subsidies from the Chinese government.[14] And in June 2026, the U.S. Department of Defense designated TP-Link Technologies—the entity from which Defendant claims it wasn't separate from until 2024—a Chinese military company operating directly or indirectly in the U.S.[15]

---

[13] TP-Link, Fact Sheet, https://www.tp-link.com/us/landing/fact-sheet/ (last visited Oct. 6, 2026), archived at https://perma.cc/9LWY-L3NU.

[14] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China*, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china.

[15] Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35193 (June 10, 2026) (designating TP-Link Technologies Co., Ltd.); U.S. Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (June 8, 2026), https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF.

11. TP-Link also represents that it manufactures its products for the U.S. market in its own factory in Vietnam, and that manufacturing in its own facilities "provides another layer of security and governance for the supply chain."[16] In truth, only 0.5% of the components in TP-Link's Vietnamese plant by value are bought in Vietnam—all other inputs are imported from or through China. Additionally, a U.S.-designated Chinese military company performed recent construction at the Vietnam factory, further evidencing the deceptiveness of TP-Link's assurances of additional security based on its Vietnam activities.[17]

12. *Second*, TP-Link deceives consumers into thinking their routers are secure, when this is not the case. TP-Link's routers have contained critical, actively exploited firmware vulnerabilities. These security vulnerabilities were exploited by Chinese state hackers to weaponize consumers' routers in the Volt and Flax Typhoon

---

[16] TP-Link, Fact Sheet, https://www.tp-link.com/us/landing/fact-sheet/ (last visited Oct. 6, 2026), archived at https://perma.cc/9LWY-L3NU; *see also* TP-Link, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (Mar. 5, 2025) ("TP-Link manufactures our routers in Vietnam in our own facility, while others in our segment continue to outsource manufacturing to Chinese original design manufacturers."), https://www.tp-link.com/us/press/news/21656/, archived at https://perma.cc/U5HT-36AN.

[17] TP-Link, Fact Sheet, https://www.tp-link.com/us/landing/fact-sheet/ (last visited Oct. 6, 2026), archived at https://perma.cc/9LWY-L3NU; Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China*, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china; Kate O'Keeffe, *Wi-Fi Giant's Vietnam Factory Raises Questions Over China Split*, Bloomberg (Nov. 22, 2025), https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split; Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35191 (June 10, 2026) (designating China State Construction Engineering Corporation Limited).

attacks according to congressional testimony. As Rob Joyce, the former Director of Cybersecurity of the National Security Agency, testified, "TP-Link routers were among the various brands exploited by Chinese state-sponsored hackers" in various attacks.[18]

13. Microsoft has likewise reported that a covert network comprised predominantly of compromised TP-Link routers has been used by Chinese threat actors to conduct credential-theft attacks against American organizations.[19]

14. Nor are Chinese state actors the only ones exploiting TP-Link's insecure routers. According to the Federal Bureau of Investigation ("FBI") and the National Security Agency ("NSA"), the Russian intelligence agency known as the GRU has exploited a critical vulnerability in TP-Link's TL-WR940N router to conduct adversary-in-the-middle attacks—attacks in which a consumer believes he or she is securely communicating with services such as Microsoft Outlook Web Access while the GRU views the traffic unencrypted.[20]

---

[18] End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, 119th Cong. (March 5, 2025) (statement of Rob Joyce), https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf.

[19] Microsoft Threat Intelligence, Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network, Microsoft (October 31, 2024), https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/.

[20] Nat'l Sec. Agency, NSA Supports FBI in Highlighting Russian GRU Threats Against Routers (Apr. 7, 2026), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/; Fed. Bureau of Investigation, Russian GRU

15. TP-Link's deception regarding security also extends to default settings—which for many routers, including the Archer AX21 v1 and v1.20, do not support automatic firmware updates. TP-Link no longer provides updates for the AX21 v1 and v1.20 at all, contending that these models reached "end of life" in May 2024.[21]

16. *Third*, in its privacy policies, TP-Link reserves the right not only to collect Floridians' personal data—including email addresses, location, and mobile phone identifiers—but also to share that data with "affiliates" to "comply with applicable laws" and to protect the rights of "others."[22] TP-Link's conduct is deceptive because it does not disclose its Chinese affiliations and the impact of the 2017 Chinese National Intelligence Law that may expose any collected or shared data to potential access by People's Republic of China ("PRC") intelligence agencies under PRC law.

17. The federal government has taken notice. The U.S. Departments of Commerce, Defense, and Justice have reportedly opened investigations into TP-

---

Exploiting Vulnerable Routers to Steal Sensitive Information, Alert No. I-260407-PSA (Apr. 7, 2026), https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF.

[21] TP-Link, End of Life Products (FAQ No. 3562), https://www.tp-link.com/us/support/faq/3562/ (last updated Sept. 18, 2026) (linking the EOL List for Home Network); TP-Link, End-of-Life Policy, https://privacy.tp-link.com/web/website/policy (last visited Oct. 6, 2026) ("TP-Link discontinues support and maintenance, including security updates, for such products."), https://perma.cc/YC7X-M7NE.

[22] TP-Link, Tether Privacy Policy (August 20, 2026), https://privacy.tp-link.com/app/Tether/privacy; TP-Link, Deco Privacy Policy (January 5, 2026), https://privacy.tp-link.com/app/Deco/privacy; TP-Link, Tapo Privacy Policy (January 23, 2026), https://privacy.tp-link.com/app/tapo/privacy (each last visited Oct. 6, 2026).

Link,[23] and federal officials have weighed banning the sale of TP-Link routers in the United States as an "unacceptable risk" to national security.[24] In March 2026, the FCC's Public Safety and Homeland Security Bureau announced the addition of routers produced in foreign countries to the FCC's Covered List, and it has since been reported that TP-Link is seeking conditional FCC approval to sell new router models in the United States.[25]

18. TP-Link's conduct has placed Florida consumers at risk of harm by making their home and small-office networks vulnerable to exploitation and intrusion by foreign actors with a proven track record of nefarious conduct. That risk is ongoing: many consumers keep their routers for years, and many of the compromised TP-Link models in Florida homes do not support automatic firmware updates and no longer receive security support at all.[26]

---

[23] Heather Somerville, Dustin Volz, and Aruna Viswanatha, *U.S. Weighs Ban on China-Made TP-Link Routers*, The Wall Street Journal (December 18, 2024).

[24] Kate O'Keeffe, Josh Sisco, and Kate Sullivan, *US Weighs Action Against China-Linked Router Giant TP-Link*, Bloomberg (October 9, 2025).

[25] FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List, WC Docket No. 18-89, Public Notice, DA 26-278 (Mar. 23, 2026), https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf; Michael Kan, *Facing Router Ban, TP-Link Tells FCC It's Investing Hundreds of Millions in the US*, PCMag (Apr. 23, 2026), https://www.pcmag.com/news/facing-router-ban-tp-link-tells-fcc-its-investing-hundreds-of-millions.

[26] Nicholas De Leon, *How to Tell When It's Time to Replace Your Router*, Consumer Reports (Apr. 30, 2021), https://www.consumerreports.org/electronics-computers/wireless-routers/how-to-tell-when-its-time-to-replace-your-router-a5475786635/ (last visited Oct. 6, 2026) (quoting Richard Fisco, who oversees electronics testing for Consumer Reports, as stating that "consumers hold onto their router for dear life and for as long as possible").

19. Accordingly, the Attorney General brings this action to enjoin TP-Link's unlawful practices; obtain appropriate relief for Florida consumers; and protect Floridians from having their privacy and security further jeopardized by TP-Link's deceptive, unfair, and unconscionable acts. The Attorney General seeks disgorgement, civil penalties, and any other relief to which the Attorney General is entitled.

PARTIES

20. Plaintiff Office of the Attorney General, State of Florida, Department of Legal Affairs (the "Attorney General") brings this action in the public interest as the enforcing authority of FDUTPA.

21. The Attorney General is the chief legal officer of the State of Florida, Fla. Const. Art. IV, § 4(b), and is expressly authorized to bring actions and obtain legal, equitable, and statutory relief as the enforcing authority under FDUTPA. §§ 501.203(2), 501.207, 501.2075, Fla. Stat.

22. Defendant TP-Link Systems Inc. ("TP-Link" or "Defendant") is a for-profit corporation organized under the laws of the State of California and is a foreign corporation for purposes of Florida law. Defendant has identified its corporate headquarters as being located at 10 Mauchly, Irvine, CA 92618,[27] and its principal address as 5 Peters Canyon Road, Suite 300, Irvine, CA 92606.[28]

---

[27] TP-Link, Corporate Information, https://www.tp-link.com/us/about-us/corporate-information/ (last visited Oct. 6, 2026), https://perma.cc/UKZ5-79Z8.

[28] Cal. Sec'y of State, Business Search, https://bizfileonline.sos.ca.gov/search/business (search "TP-Link" and click on TP-Link Systems Inc.) (last visited Oct. 6, 2026).

23. TP-Link transacts business in Florida by marketing, offering, and selling TP-Link routers and other devices, and related applications and services, to Florida consumers.

24. At all relevant times, Defendant acted directly and through its affiliates, agents, subsidiaries, contract manufacturers, and related entities—which acted with Defendant's knowledge, at its direction, under its control, and for its benefit—to design, advertise, promote, import, distribute, and sell TP-Link devices in Florida. Defendant is responsible for the deceptive, unfair, and unconscionable acts and practices alleged in this Complaint, including those carried out by or through those entities.

25. Unless otherwise specified, this Complaint uses "TP-Link" to refer to Defendant TP-Link Systems Inc. and, as to conduct predating the corporate restructuring described below, to the TP-Link enterprise from which Defendant was allegedly carved out and whose United States business, brand, product lines, marketing, and customer relationships Defendant assumed and continues to operate. "TP-Link Technologies" refers to TP-Link Technologies Co., Ltd., a Chinese entity that is not a party to this action. Defendant is responsible for the representations and omissions alleged here.

JURISDICTION AND VENUE

26. This is an action for injunctive relief, other equitable relief, civil penalties, and other statutory relief, brought pursuant to FDUTPA.

27. Defendant's statutory violations occurred in or affect more than one judicial circuit in the State of Florida, including the Tenth Judicial Circuit in and for Polk County.

28. This Court has subject matter jurisdiction over the claims at issue under Section 501.207(3), Florida Statutes.

29. The Attorney General is the enforcing authority of FDUTPA under Section 501.203(2), Florida Statutes, because the violations alleged in this Complaint occurred in, and have affected consumers in, more than one judicial circuit of the State of Florida.

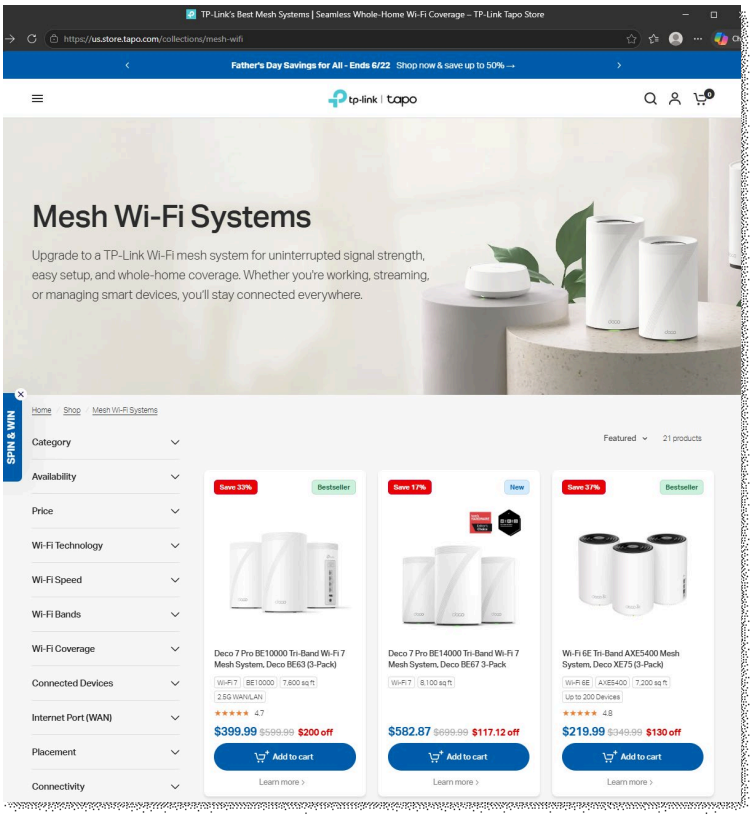
30. The Attorney General has reviewed the matters alleged here and has determined that this enforcement action serves the public interest.

31. At all times material here, Defendant engaged in "trade or commerce" within the meaning of Section 501.203(8), Florida Statutes, by advertising, soliciting, providing, offering, and distributing goods and services—including routers, other devices, and related applications and services—to consumers in Florida.

32. TP-Link at all relevant times directly offered and sold routers and other products to Florida consumers through its own online websites, including https://us.store.tp-link.com and https://us.store.tapo.com/. On information and belief, TP-Link collects users' "location" when they interact with its store.[29]

[29] https://us.store.tapo.com/pages/privacy-policy (Jan. 1, 2020), archived at https://perma.cc/3L7Y-8EQJ

33. For example, TP-Link directly sells its Deco mesh router systems to consumers in Florida.[30]



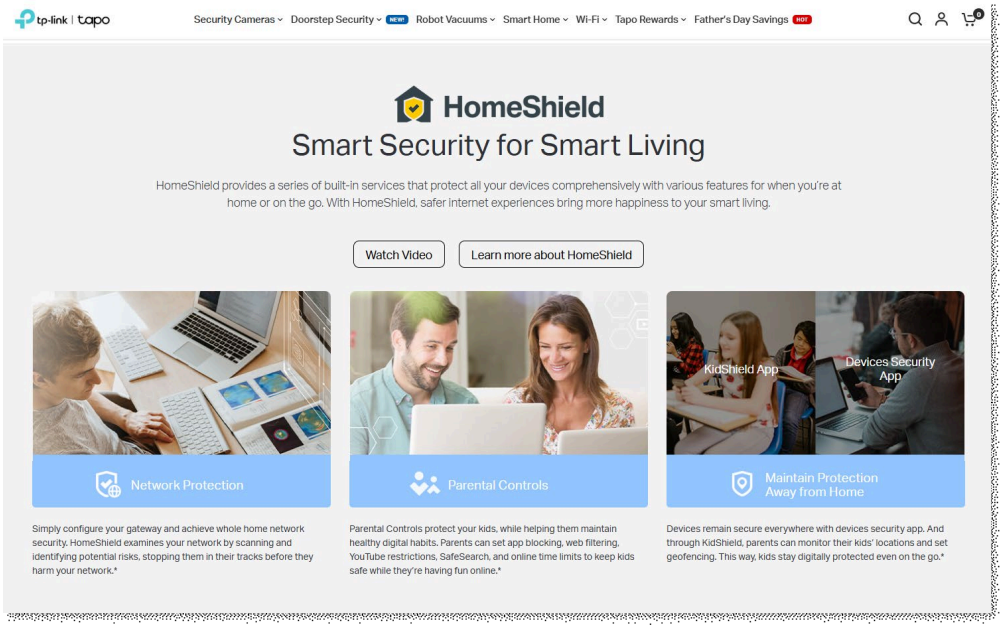
34. These offers and sales also involve TP-Link specifically touting both its HomeShield service and its various apps, such as its Tether App.[31]

---

[30] TP-Link, Deco Mesh Wi-Fi Systems, TP-Link Store, https://us.store.tapo.com/collections/mesh-wifi (last visited Oct. 6, 2026), archived at https://perma.cc/2CAV-E297.

[31] TP-Link, HomeShield & Tether App, TP-Link Store, https://us.store.tp-link.com (last visited Oct. 6, 2026), archived at https://perma.cc/4HNX-YWG5.

TP-Link HomeShield: TP-Link's premium security service keeps your home network safe with cutting-edge network and IoT protection. Free features: 1) Basic Network Security including Security Scan and IoT Device Identification; 2) Basic Parental Controls; 3) Quality of Service; 4) Basic Weekly/Monthly Reports. Visit TP-Link's website for more information.



35. As discussed below, TP-Link's statements regarding these products and services—which it directly sells to Florida consumers—are unfair and deceptive and violate FDUTPA.

36. TP-Link also sells its products and services to Florida consumers through online and physical retailers. These retailers include BrandsMart USA, Office Depot, Amazon, Best Buy, Costco, Walmart, Target, Home Depot, Lowe's, Sam's Club, Staples, and others.[32]

[32] https://www.tp-link.com/us/where-to-buy/ (last visited Oct. 6, 2026), archived at https://perma.cc/L2UB-G2HH.

37. BrandsMart USA is one of the retailers that TP-Link prominently lists. It is headquartered in Opa-locka in Miami-Dade County.[33] Eight of its eleven stores are in Florida.[34]

38. OfficeDepot is another retailer that TP-Link prominently lists. It opened its first store in Fort Lauderdale[35] and is headquartered in Boca Raton.[36]

39. Advanced Media Technologies ("AMT") is a distributor that TP-Link prominently lists. AMT is headquartered at Deerfield Beach.[37]

40. TP-Link also sells to internet service providers ("ISPs") that operate in primarily or entirely in Florida, including Blue Stream Fiber, Broadstar, Central Florida Broadband, QXC Communications, Summit Broadband, and WingNet Communications.

41. TP-Link also directly offers applications such as TP-Link Tether, TP-Link Tapo, TP-Link Deco, and Kasa Smart on Apple's App Store and Google's Play Store to Florida consumers.[38] In addition, the Apple and Google Play stores indicate

---

[33] https://www.linkedin.com/company/mobile-electronics-inc.net/home/ (last visited Oct. 6, 2026).

[34] *See generally* https://www.brandsmartusa.com/pages/about-brandsmart-usa (last visited Oct. 6, 2026).

[35] https://www.officedepot.com/specialLinks.do?desktop=true&file=%2Fcompanyinfo%2Fcompanyfacts%2Fcompanyhistory.jsp&template=companyInfo (last visited Oct. 6, 2026).

[36] https://www.linkedin.com/company/office-depot/home/ (last visited Oct. 6, 2026).

[37] https://amt.com/company/ (last visited Oct. 6, 2026).

[38] Google Play Store for Android, TP-Link Tether, https://play.google.com/store/apps/details?id=com.tplink.tether&hl=en_US (last visited Oct. 6, 2026); App Store for iPhone, Kasa Smart, https://apps.apple.com/us/app/kasa-smart/id1034035493 (last visited Oct. 6, 2026).

that these programs also involve "in-app purchases" by consumers. TP-Link sells TapoCare and KasaCare subscriptions to consumers.[39] When a user enables "Geofencing Smart Action," TP-Link collects the user's precise location.[40] TP-Link sells its software to consumers knowing that they are located in Florida.

42. This Court has personal jurisdiction over Defendant under Florida's long-arm statute, Section 48.193(1)(a), Florida Statutes. The cause of action arises from TP-Link (1) "[o]perating, conducting, engaging in, or carrying on a business or business venture in this state or having an office or agency in this state"; (2) "[c]ommitting a tortious act within this state"; and (6) "[c]ausing injury to persons or property within this state arising out of an act or omission by the defendant outside this state" where, at or about the time of the injuries, TP-Link was engaged in solicitation or service activities in Florida and its products were used or consumed in Florida in the ordinary course of commerce.

43. Defendant purposefully availed itself of the privilege of conducting business in Florida by advertising and selling thousands of devices to consumers in Florida, as well as software to consumers in Florida. The conduct and injuries from which this Complaint arises took place in Florida, harmed Floridians, and targeted Floridians.

---

[39] https://www.tapo.com/us//tapocare/; https://www.kasasmart.com/us/kasacare

[40] https://privacy.tp-link.com/app/tapo/privacy, archived at https://perma.cc/2WCP-EKEB.

44. The Attorney General brings this action exclusively under the laws of the State of Florida. No federal claims are being asserted, and to the extent that any claim or factual assertion set forth here may be construed to have stated any claim for relief arising under federal law, such claim is expressly disavowed and disclaimed.

45. Venue is proper because the allegations in this Complaint establish that the causes of action here accrued in Polk County. See Section 47.051, Florida Statutes.

FACTUAL ALLEGATIONS

I. TP-Link Is a China-Founded Company That Remains Dependent on China in Critical Ways

46. TP-Link is a global provider of networking and smart home devices for consumers and small to mid-size organizations. TP-Link was founded in 1996 by brothers Zhao Jiaxing ("Cliff Chao") and Zhao Jianjun ("Jeffrey Chao") in Shenzhen, China, and expanded into the United States market in 2008 by establishing TP-Link USA. By 2016, TP-Link Technology's reported global revenues (which included the U.S. market) exceeded $2 billion.

47. TP-Link is a dominant player in the United States' networking and smart home technology market. According to congressional testimony, TP-Link has a 60 percent or greater share of the United States consumer retail market for Wi-Fi systems and small-office/home-office routers.[41] TP-Link's smartphone applications

[41] End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, 119th Cong. (2025), (statement of Rob Joyce).

are ranked among the top downloads in Apple's App Store "Utilities" category, and TP-Link's sponsored Amazon listings show tens of thousands of monthly purchases.

48. After more than a decade in the U.S. market, TP-Link announced it had restructured the company into two distinct operations. By 2024, Cliff Chao retained operating control of TP-Link's Chinese sales through the entity TP-Link Technologies, and Jeffrey Chao became the CEO and owner of Defendant TP-Link Systems Inc. ("TP-Link"). TP-Link represented to Floridians that this divide "encompass[ed] all shareholdings and operational aspects, including legal entities, workforce, research and development, production, marketing, and customer service."[42]

49. In March 2025, TP-Link again represented to Floridians that it had "entirely different ownership, management, and operations" than TP-Link Technologies. [43] TP-Link also presently represents that "[a]s a company headquartered in the United States, no government—foreign or domestic—has access to and control over the design and production of our routers and other devices."[44]

---

[42] TP-Link, TP-Link Corporation Group Announces Completion of Corporate Restructuring, Marking a New Era in Its Future Evolution (May 11, 2024), https://www.tp-link.com/us/press/news/21130/, archived at https://perma.cc/R7D8-FSRM.

[43] TP-Link, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (March 5, 2025), https://www.tp-link.com/us/press/news/21656/, archived at https://perma.cc/U5HT-36AN.

[44] TP-Link, Fact Sheet, https://www.tp-link.com/us/landing/fact-sheet/ (last visited Oct. 6, 2026), archived at https://perma.cc/9LWY-L3NU.

50. Despite its representation that it had completely separated from China, TP-Link admits elsewhere that it "still has substantial operations in mainland China."[45]

51. In fact, the scale of TP-Link's remaining Chinese operations dwarfs its U.S. presence. According to Bloomberg News, the operations of TP-Link and TP-Link Technologies in China employ approximately 11,000 people, compared to roughly 305 employees based in the United States. Bloomberg reported that "much of the research, development and manufacturing operations of [the] new U.S. company remain in China, entrenched in the country's state-sponsored technology ecosystem, despite the restructuring."[46] The relatively low number of U.S. employees is consistent with current statistics on LinkedIn, which show only 484 associated members, defined as "LinkedIn members who've listed TP-Link Systems Inc. as their current workplace on their profile."[47] One former employee wrote on Glassdoor.com in June 2026, that "Despite efforts to present itself as an American employer, my experience was that TP-Link remains fundamentally a Chinese company operating in the United States. ... U.S.-based leaders often appeared to have less authority than their titles suggested, with major decisions ultimately controlled elsewhere.

[45] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China*, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china.

[46] *Id.*

[47] https://www.linkedin.com/company/tp-link/about/

Transparency was limited, organizational changes were frequent, and priorities often shifted without clear explanation."[48]

52. TP-Link has operational control over at least four major facilities in China used to manufacture, research, and develop its devices: TP-Link's Shenzhen Research and Development Center, Shenzhen Manufacturing Center, Dongguan Manufacturing Center, and Shenzhen Guangqiao Manufacturing Center. Further, TP-Link is building a fifth engineering facility in Chengdu, China.[49]

53. TP-Link has implicitly admitted its continuing Chinese investments. When asked by Bloomberg in April 2025 about an $180 million investment in the Chengdu engineering facility, TP-Link's spokesperson stated only that the company "has currently stopped increasing its investments in personnel, R&D, and manufacturing in China." A purported policy to stop increasing investments is not a separation of "all ... operational aspects, including ... research and development [and] production," as TP-Link represented to the public.[50]

---

[48] https://www.glassdoor.com/Reviews/Employee-Review-TP-Link-Systems-Inc-E10762893-RVW104415054.htm, archived at https://perma.cc/WNP2-F23R.

[49] TP-Link, 2024 Sustainability Report, https://static-page.tp-link.com/sustainability/pdf/TP-Link%202024%20Sustainability%20Report.pdf (last visited Oct. 6, 2026).

[50] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China, Bloomberg* (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china; TP-Link, TP-Link Corporation Group Announces Completion of Corporate Restructuring, Marking a New Era in Its Future Evolution (May 11, 2024), https://www.tp-link.com/us/press/news/21130/.

54. Jeffrey Chao has admitted that TP-Link's Chinese facilities and subsidiaries have "recently received state accolades and benefits."[51] The Chinese government uses subsidies, such as lucrative tax breaks, free land, and expedited permitting for industrial facilities.[52]

55. That relationship—and dependence—runs deeper than financial support. Hunan, a Chinese province, announced that TP-Link's Vietnamese factory was one of its "Key Projects for Foreign Investment and Cooperation." The notice reportedly identified a company—which the U.S. government has designated as a Chinese military company—as working to expand TP-Link's manufacturing, research, and development facilities in Vietnam.[53]

56. In June 2026, the U.S. Department of Defense identified TP-Link Technologies—the Chinese entity from which Defendant claims complete separation—as a Chinese military company operating directly or indirectly in the United States under Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.[54]

---

[51] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China*, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china.

[52] Christine Clark, *Accelerating the Energy Revolution by Working with China*, UC San Diego Today (June 18, 2024), https://today.ucsd.edu/story/accelerating-the-clean-energy-revolution-by-working-with-china, (last visited Oct. 6, 2026).

[53] Kate O'Keeffe, *Wi-Fi Giant's Vietnam Factory Raises Questions Over China Split*, Bloomberg (November 22, 2025), https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split.

[54] Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35193 (June 10, 2026) (designating TP-Link Technologies Co., Ltd.); U.S.

57. Even after TP-Link represented to Florida consumers that it completely split from TP-Link Technologies, representatives of both companies reportedly attended a Chinese Communist Party event together in China and posted a photograph on social media showing the two employees standing next to each other under the party's hammer-and-sickle emblem, each holding "TP-Link" signs bearing their respective corporate logos.[55]

58. Reporting and trade data show that TP-Link has imported items into the United States from China for years. TP-Link's shipments from Lianzhou Technologies Co., Ltd. have departed from China to Long Beach, California, as recently as January 2026. On information and belief, TP-Link Systems Inc. has imported shipments from its Chinese-affiliated companies, such as TP-Link Technologies and Lianzhou Technologies Co., Ltd.[56]

Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (June 8, 2026), https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF.

[55] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China*, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china.

[56] ImportGenius, Lianzhou Technologies Co., Ltd., https://www.importgenius.com/suppliers/lianzhou-technologies-co-ltd (last visited Oct. 6, 2026); ImportInfo, TP-LINK SYSTEMS INC, https://www.importinfo.com/tp-link-systems-inc (last visited Oct. 6, 2026); ImportInfo, TP-LINK USA CORPORATION, https://www.importinfo.com/tp-link-usa-corporation (last visited Oct. 6, 2026).

59. On information and belief, TP-Link also uses TP-Link USA Corporation to import from China. According to trade information, TP-Link USA Corporation has had shipments from Shanghai, China as recently as December 2025.[57] This further shows TP-Link's connection to China regardless of the corporate entity used to receive the goods.

II. China's Legal Regime Compels Cooperation with PRC Intelligence, Including Nearly Contemporaneous Disclosure of Zero-Day Security Vulnerabilities

60. The U.S. government has designated China a foreign adversary of the United States. 15 C.F.R. § 791.4.

61. Article 7 of China's 2017 National Intelligence Law requires that Chinese organizations and citizens "support, assist, and cooperate with national intelligence efforts in accordance with law" and "protect national intelligence work secrets they are aware of." Article 14 of the same law provides that Chinese intelligence institutions "may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[58]

62. United States Department of Homeland Security ("DHS") has warned American businesses that this law "forms the baseline of the modern data collection regime, and compels all PRC firms and entities to support, assist, and cooperate with

---

[57] ImportInfo, TP-LINK USA CORPORATION, https://www.importinfo.com/tp-link-usa-corporation, (last visited Oct. 6, 2026).

[58] PRC National Intelligence Law arts. 7, 14 (as amended 2018), China Law Translate (June 27, 2017), https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/; see https://cs.brown.edu/courses/cs180/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf.

the PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC." DHS further explained that the law "establishes a system of incentives for compliance and penalties for non-compliance," including that a person who "obstructs ... state intelligence work" "shall be dismissed, investigated and/or detained."[59]

63. Under China's 2021 RMSV, Chinese network-product providers and network operators must report newly discovered security vulnerabilities to China's Ministry of Industry and Information Technology within a mere two days of discovery. A senior DHS official has stated that the Chinese government appears to use this vulnerability-disclosure rule to preview dangerous zero-day flaws before technology companies can deploy fixes.[60]

64. The risks from these laws matter to Florida consumers. A company whose research, development, manufacturing, personnel, and affiliates are subject to this regime cannot truthfully assure consumers that their routers, networks, and personal data are protected from "any" cyber threats, or that "no government" has access to or control over the design and production of its devices.

---

[59] U.S. Dep't of Homeland Sec., Data Security Business Advisory 6 (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[60] Stewart Scott et al., Dragon Tails: Preserving International Cybersecurity Research, Atlantic Council (Sept. 2022), https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/; Suzanne Smalley, China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says, CyberScoop (Aug. 10, 2022), https://cyberscoop.com/dhs-official-chinese-rules-exploit/ (reporting remarks of DHS Under Secretary for Policy Robert Silvers).

III. TP-Link's Representations That It Separated from China and Manufactures Its Product in Vietnam Are Deceptive and Omit Material Information

65. TP-Link represents that it "manufacture[s] products for the U.S. market in its own factory in Vietnam" and that "[m]anufacturing products in TP-Link facilities with our own employees provides another layer of security and governance for the supply chain serving the U.S. market and beyond."[61] In a 2023 announcement, TP-Link claimed that "all product manufacturing" related to its smart home products was handled by its Vietnamese entity Lianyue Vietnam Co. Ltd.[62]

66. In 2025, after the House Select Committee on the Chinese Communist Party held a hearing discussing TP-Link's relation to Chinese state-sponsored cyberattacks, TP-Link represented that it "manufactures [its] routers in Vietnam in [its] own facility."[63]

67. The reality behind TP-Link's Vietnamese manufacturing claims tells a different story. Only 0.5% of the components used in TP-Link's Vietnamese factory by value are bought in Vietnam; all other inputs are imported from or through China. Bloomberg reported this figure based on trade data, and TP-Link confirmed it.[64]

---

[61] TP-Link, Fact Sheet, https://www.tp-link.com/us/landing/fact-sheet/ (last visited Oct. 6, 2026), archived at https://perma.cc/9LWY-L3NU.

[62] TP-Link, BFG Group Announcement (September 19, 2023).

[63] TP-Link, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (Mar. 5, 2025), https://www.tp-link.com/us/press/news/21656/, archived at https://perma.cc/U5HT-36AN.

[64] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China*, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china; Kate O'Keeffe, *Wi-Fi Giant's Vietnam Factory Raises Questions Over China Split*, Bloomberg (Nov. 22, 2025),

68. TP-Link's Vietnam facility also has connections to the Chinese military. TP-Link recently used a construction contractor for its Vietnam plant—China State Construction Engineering Corporation—that the U.S. Department of Defense has designated a Chinese military company.[65]

69. TP-Link omits material facts to deceive consumers into thinking its Vietnamese-assembled products and its supply chain are unaffiliated with China, a designated foreign adversary. The reality is that TP-Link continues to operate its supply chain with deep Chinese connections, Chinese governmental support, and Chinese exports. The final assembly of components sourced from or through China in Vietnam does not cure the company's deceptive statements and material omissions regarding its Chinese dependence and affiliations.

IV. TP-Link Makes False and Deceptive Security Representations While Its Routers Have Been Repeatedly Exploited in Serious Cyberattacks

70. TP-Link represents to consumers that its networking devices robustly protect their privacy and security. Those representations are false or deceptive.

A. The TP-Link TL-WR940N and Archer C7 Routers: Exploited by the Quad7 Botnet and the Russian GRU

71. TP-Link advertised its TL-WR940N router as providing "[e]asy wireless security encryption at a push of [a] WPS button" and "Easy Setup and Use," and

---

https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split.

[65] Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35191 (June 10, 2026) (designating China State Construction Engineering Corporation Limited); see also Kate O'Keeffe, *Wi-Fi Giant's Vietnam Factory Raises Questions Over China Split*, Bloomberg (Nov. 22, 2025), https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split.

represented that its Tether app "lets you manage [the router's] network settings ... including ... access control." TP-Link sold versions of this router through 2024, and on information and belief many Florida consumers still use it.[66]

72. Contrary to TP-Link's representations, the TL-WR940N contained a critical vulnerability. TP-Link has admitted that CVE-2023-50224 affects the TL-WR940N. This vulnerability has been exploited by the operators of the Quad7 botnet—tracked by Microsoft as CovertNetwork-1658 and attributed by Microsoft to Chinese threat actors—and by Russia's GRU.[67]

---

[66] TP-Link, TL-WR940N Product Page (archived Mar. 29, 2023), https://web.archive.org/web/20230329192916/https://www.tp-link.com/us/home-networking/wifi-router/tl-wr940n/; TP-Link, FAQ No. 5058 (last updated May 12, 2026), https://www.tp-link.com/us/support/faq/5058/, archived at https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/ and https://perma.cc/XRK7-WA3J; see also https://perma.cc/F4B2-UR85, at 55 (listing end of sale of the TL-WR940N v6 plus model as Apr. 23, 2024).

[67] TP-Link, Press Release No. 22295, *An Important Update for TP-Link Customers Regarding Recent CVE-2023-50224 Reporting* (May 1, 2026), https://www.tp-link.com/us/press/news/22295/; Nat'l Inst. of Standards & Tech., CVE-2023-50224 Detail, National Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-50224 (last visited Oct. 6, 2026); TP-Link, FAQ No. 5058 (last updated May 12, 2026), https://www.tp-link.com/us/support/faq/5058/, archived at https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/ and https://perma.cc/XRK7-WA3J (identifying CVE-2023-50224 as applicable to the TL-WR940N); Fed. Bureau of Investigation, Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information, Alert No. I-260407-PSA (Apr. 7, 2026), https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF; Microsoft Threat Intelligence, Chinese Threat Actor Storm-0940 Uses Credentials from Password Spray Attacks from a Covert Network, Microsoft (Oct. 31, 2024), https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/; TP-Link, FAQ No. 4365 (archived Jan. 26, 2025), https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/.

73. Microsoft reported in October 2024 that CovertNetwork-1658—comprised predominantly of compromised TP-Link routers—was used to conduct "highly evasive password spray attacks" against targets including "think tanks, government organizations, non-governmental organizations, law firms, [and the] defense industrial base," and that a Chinese threat actor known as Storm-0940 used credentials obtained from those attacks to intrude into targeted organizations. Password spraying is when a hacker attempts to gain unauthorized access by using a password across several accounts at once. TP-Link itself acknowledged that "the Quad 7 ... botnet ... is used by Chinese threat actors for password spray attacks against Microsoft 365 accounts," that "[t]he threat actor exploits vulnerabilities in the routers to gain remote code execution capability," and that the network is "predominantly TP-Link devices."[68] This overlap is itself material and undisclosed: in June 2026, the U.S. Department of Defense identified TP-Link Technologies, Hangzhou Hikvision Digital Technology Co., Ltd., and Zhejiang Dahua Technology Co., Ltd.—all three compromised in the same overall botnet—as Chinese military companies, a civil-military-fusion connection TP-Link deceptively omits despite touting its routers' security.[69]

---

[68] Microsoft Threat Intelligence, Chinese Threat Actor Storm-0940 Uses Credentials from Password Spray Attacks from a Covert Network, Microsoft (Oct. 31, 2024), https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/; TP-Link, FAQ No. 4365 (archived Jan. 26, 2025), https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/.

[69] Gi7w0rm, The Curious Case of the 7777 Botnet, Medium (Oct. 19, 2023), https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd,

74. The FBI and NSA report that the Russian GRU has exploited compromised routers to conduct adversary-in-the-middle attacks: "[t]he GRU provides fraudulent DNS [Domain Name System] answers for specific domains and services—including Microsoft Outlook Web Access—enabling adversary-in-the-middle (AitM) attacks against encrypted traffic if users navigate through a certificate error warning." In other words, a consumer would believe he or she is securely communicating with Outlook Web Access while the unencrypted content of the traffic is disclosed to the GRU.[70]

75. The TL-WR940N does not have proper "access control"—it allows unauthorized actors to gain administrator access and conscript the router into an illegal botnet. Nor is it "[e]asy [to] [s]etup and [u]se": the router does not support

---

archived at https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd; Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35192–94 (June 10, 2026) (designating Hangzhou Hikvision Digital Technology Co., Ltd., TP-Link Technologies Co., Ltd., and Zhejiang Dahua Technology Co., Ltd.); U.S. Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (June 8, 2026), https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF.

[70] Nat'l Sec. Agency, NSA Supports FBI in Highlighting Russian GRU Threats Against Routers (Apr. 7, 2026), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/; Fed. Bureau of Investigation, Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information, Alert No. I-260407-PSA (Apr. 7, 2026), https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF.

automatic firmware updates, so protecting it requires manually installing a patch that many users would not know to install.[71]

76. TP-Link's conduct after this vulnerability became public compounded the deception. In April 2026, TP-Link published a list of routers affected by these attacks that omitted the TL-WR940N and stated that "[a]ll the affected products have reached End-of-Life (EOL) status and [are] no longer within TP-Link's standard maintenance lifecycle." In May 2026, TP-Link was forced to admit that the TL-WR940N was also affected—even though a 2023 security analysis that TP-Link itself had cited specifically identified the TL-WR940N.[72]

77. TP-Link likewise advertised the Archer C7 AC1750 (versions 2 and 3) as "provid[ing] secure Wi-Fi access for guests sharing your home or office network" and offering "[e]asy setup and management with Tether App." TP-Link also promoted the Archer C7 in an online video advertisement telling consumers that purchasing

---

[71] TP-Link, FAQ No. 2796, https://www.tp-link.com/us/support/faq/2796/, archived at https://perma.cc/G6RS-2YKS (explaining how to update firmware manually).

[72] Gi7w0rm, *The Curious Case of the 7777 Botnet*, Medium (Oct. 19, 2023), https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd, archived at https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd; TP-Link, FAQ No. 4365 (archived Jan. 26, 2025), https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/ (January 2025 TP-Link article citing that report); TP-Link, FAQ No. 5058 (updated Apr. 9, 2026), archived at https://web.archive.org/web/20260410034756/https://www.tp-link.com/us/support/faq/5058/; TP-Link, FAQ No. 5058 (last updated May 12, 2026), https://www.tp-link.com/us/support/faq/5058/, archived at https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/ and https://perma.cc/XRK7-WA3J.

the router would "future-proof" their home network and reiterating that it "provides secure Wi-Fi access for guests sharing your home or office network."[73] Contrary to those representations, versions 2 and 3 of the Archer C7 were compromised in the Quad7 botnet operations, and neither version supports automatic firmware updates.[74] The Archer C7 was also one of the TP-Link Routers hacked by the Russian GRU.[75]

B. The Archer AX21: Exploited in the Flax Typhoon Attacks

78. TP-Link advertised the Archer AX21 (AX1800) router as offering "Refined Password Security" and a "New Level of Cyber Security" with the "latest Wi-Fi security protocol, WPA3," along with "easy setup." The AX21 was the bestselling Wi-Fi 6 router on Amazon, and its current version (v5) remains listed as "Amazon's Choice," underscoring the continued prominence of the AX21 product line among consumers.[76]

---

[73] TP-Link, Archer C7 Promotional Video, YouTube, https://www.youtube.com/watch?v=-PEWXGUQiQ8, at 1:00 ("future-proof"), 1:54 ("secure Wi-Fi access for guests").

[74] TP-Link, Archer C7 Product Page (archived Mar. 31, 2026), https://web.archive.org/web/20260331134655/https://www.tp-link.com/us/home-networking/wifi-router/archer-c7/; TP-Link, FAQ No. 5058, https://www.tp-link.com/us/support/faq/5058/; see generally TP-Link, FAQ No. 2796, https://www.tp-link.com/en/support/faq/2796/.

[75] FBI Says Russian Hackers Hijacked Old Wi-Fi Routers, Fox News (June 14, 2026), https://www.foxnews.com/tech/fbi-says-russian-hackers-hijacked-old-wi-fi-routers.amp

[76] TP-Link, Archer AX21 Product Page (archived Oct. 6, 2022), https://web.archive.org/web/20221006205422/https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/; *Forget Slow WiFi, Amazon Just Cut the Best-Selling WiFi 6 TP-Link Router to a Near Record Low*, Gizmodo (May 10, 2026), https://gizmodo.com/forget-slow-wifi-amazon-just-cut-the-best-selling-wifi-6-tp-link-router-to-a-near-record-low-2000756849; TP-Link AX1800 Wi-Fi 6 Router

79. In 2023, it was publicly disclosed that versions 1 through 3 of the AX21 contained a critical vulnerability, CVE-2023-1389, allowing an unauthenticated attacker—i.e., an attacker that does not know the router's password—to nonetheless inject malicious commands. TP-Link admitted in April 2023 that the "AX21 has been added to the Mirai botnet Arsenal." The vulnerability has been actively exploited by multiple botnet operations, including by the Chinese state-affiliated Flax Typhoon group, whose botnet the FBI ultimately disrupted on information and belief through a court-authorized operation remotely resetting thousands of compromised routers.[77]

80. TP-Link's marketing created a false impression of security for consumers: a router advertised for "Refined Password Security" allowed attackers to gain root access with no password at all.

(ArcherAX21 V5), Amazon, https://www.amazon.com/WiFi-6-Router-Gigabit-Wireless/dp/B08H8ZLKKK (last visited Oct. 6, 2026).

[77] Nat'l Inst. of Standards & Tech., CVE-2023-1389 Detail, National Vulnerability Database, https://nvd.nist.gov/vuln/detail/cve-2023-1389 (last visited Oct. 6, 2026); SentinelOne, CVE-2023-1389, SentinelOne Vulnerability Database, https://www.sentinelone.com/vulnerability-database/cve-2023-1389/; https://perma.cc/BNC8-C69P (TP-Link statement that the "AX21 has been added to the Mirai botnet Arsenal"); Router Security by the Numbers: 10 Years of CVE Data, 5Gstore Blog (Apr. 12, 2026), https://5gstore.com/blog/2026/04/12/router-security-by-the-numbers-10-years-of-cve-data/; Lulzim A., *FBI Remotely Resets Thousands of Routers to Disrupt Flax Typhoon Botnet*, RouterArena, https://routerarena.com/news/FBI-remotely-resets-thousands-of-routers-to-disrupt-Flax-Typhoon-botnet; *see also* Daryna Antoniuk, *Botnets continue exploiting year-old flaw in unpatched TP-Link routers*, The Record (Apr. 16, 2024), https://therecord.media/tp-link-router-vulnerability-botnets; Elizabeth Montalbano, *Emerging botnet exploits TP-Link router flaw posing risk to US organizations*, Cybersecurity Dive (Mar. 12, 2025), https://www.cybersecuritydive.com/news/-botnet-exploits-tp-link-router/742319/.

81. Versions 1 and 1.20 of the AX21 did not support automatic firmware updates as a default setting. To be protected, a consumer had to know about the vulnerability and manually download and install a firmware patch. And even consumers who installed TP-Link's Tether app received notice of this critical security update only as a red dot on a menu within the app. TP-Link no longer provides updates for the AX21 v1 and v1.20, contending these models reached "end of life" in May 2024. TP-Link has continued to obfuscate, claiming it "has not been able to verify how its devices are affected, if at all."[78]

C. HomeShield Does Not "Cover [] All Security Scenarios"

82. TP-Link represents that its routers, such as the Archer BE9700 router offered through national retailers that serve Florida consumers, feature "Network Security with HomeShield." HomeShield is a "built-in service" available in all HomeShield routers and Deco Mesh products that purports to provide consumers with privacy and security controls over their homes and businesses' networks. TP-Link currently represents that HomeShield "covers all security scenarios," that it handles all concerns about "cyber virus intrusion" and "IoT device attacks," and that

[78] *See generally* TP-Link, FAQ No. 2796, https://www.tp-link.com/en/support/faq/2796/ archived at https://perma.cc/G6RS-2YKS; Kate O'Keeffe, Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split from China, Bloomberg (Apr. 11, 2025), https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china.

users can "[c]heck the results of the scans and preventions against any potential cyber threats or attacks for your home network."[79]

83. TP-Link accompanies many of these representations with a graphic that specifically shows consumers a picture of a masked individual in front of a laptop with the caption "Private Info Leakage," and other pictures with the captions "Cyber Virus Intrusion" and IoT Device Attacks."[80]



84. A version of TP-Link's website available as recently as November 2025 further represented that HomeShield provides a "100% safeguard" for network security.[81]

---

[79] Current version: TP-Link, HomeShield, https://www.tp-link.com/us/homeshield/ (last visited Oct. 6, 2026), archived at https://perma.cc/M8ME-4EX7.

[80] *Id.*

[81] TP-Link, HomeShield (archived Nov. 14, 2025), https://web.archive.org/web/20251114185316/https://www.tp-link.com/us/homeshield/.

85. Consumers trust TP-Link's representations when considering which device to purchase. TP-Link knows this, and TP-Link knows of its devices' plethora of cybersecurity vulnerabilities.

86. TP-Link's HomeShield representations are belied by vulnerabilities in the very routers TP-Link advertises with HomeShield. TP-Link advertised the Archer AXE75 with HomeShield and represented that it has "advanced security features that deliver a safe environment that protects your family and network's data and privacy." Yet the AXE75 was subject to CVE-2024-53375, a high-severity vulnerability allowing an attacker to execute commands on the router, and CVE-2025-15568, which allows remote code execution in certain scenarios. As TP-Link admitted for one of these, "[s]uccessful exploitation results in root-level privileges and impacts confidentiality, integrity and availability of the device."[82] This could allow a hacker to intercept the raw packet data being transmitted through the router or redirect traffic and send a user to a malicious website. Other routers TP-Link advertises with HomeShield—including the Archer BE230, Archer AX73, and Deco BE25—were likewise subject to command-injection vulnerabilities.[83]

---

[82] TP-Link, Security Advisory on Command Injection Vulnerability on TP-Link Archer AXE75 (CVE-2025-15568), https://www.tp-link.com/us/support/faq/5005/ archived at https://perma.cc/G9J3-4SB8.

[83] TP-Link, Archer AXE75 Product Page, https://www.tp-link.com/us/home-networking/wifi-router/archer-axe75/ (last visited Oct. 6, 2026), archived at https://perma.cc/N7F3-JVCB; Nat'l Inst. of Standards & Tech., CVE-2024-53375 Detail, National Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2024-53375 (last visited Oct. 6, 2026); TP-Link, FAQ No. 5005, https://www.tp-link.com/us/support/faq/5005/; Nat'l Inst. of Standards & Tech., CVE-2025-15568 Detail, National Vulnerability Database, https://nvd.nist.gov/vuln/detail/cve-2025-

87. HomeShield also cannot address a risk that TP-Link never discloses to consumers: Even when TP-Link eventually patches a vulnerability—which can take weeks or months—later patching does not eliminate the risk that the Chinese government learns of the zero-day flaw first. Under the RMSV, described in Section II above, Chinese technology providers and network operators must report newly discovered vulnerabilities to the Chinese government within two days of discovery. A service that purports to "cover[] all security scenarios" and "handle[] all your concerns" while its provider's Chinese facilities and affiliates are subject to that regime is deceptive and omits material information from consumers.[84]

88. Former FCC Commissioner Michael O'Rielly wrote that TP-Link's "Chinese investment structures" warranted inquiry and that its products "had more than their fair share" of vulnerabilities.[85]

15568 (last visited Oct. 6, 2026); TP-Link, FAQ No. 4935, https://www.tp-link.com/us/support/faq/4935/.

[84] Stewart Scott et al., *Dragon Tails: Preserving International Cybersecurity Research*, Atlantic Council (Sept. 2022), https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/; Suzanne Smalley, China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says, CyberScoop (Aug. 10, 2022), https://cyberscoop.com/dhs-official-chinese-rules-exploit/ (reporting remarks of DHS Under Secretary for Policy Robert Silvers); TP-Link, HomeShield, https://www.tp-link.com/us/homeshield/ (last visited Oct. 6, 2026), archived at https://perma.cc/M8ME-4EX7.

[85] Michael O'Rielly, *Chinese Wireless Routers: The Next Entry Point for State-Sponsored Hackers?*, Hudson Institute (March 2024), https://s3.amazonaws.com/media.hudson.org/030724_ORielly_Chinese_Routers_Hackers_Memo.pdf.

89. Rob Joyce, the former Director of Cybersecurity of the National Security Agency, has testified that "TP-Link routers were among the various brands exploited by Chinese state-sponsored hackers" in various attacks.[86]

90. The Chairman of the United States House of Representatives' Select Committee on the Chinese Communist Party, John Moolenaar, wrote to Secretary Gina Raimondo of the United States Department of Commerce, warning of TP-Link devices' vulnerabilities and requesting an investigation: "TP-Link's unusual degree of vulnerabilities and required compliance with PRC law are in and of themselves disconcerting. When combined with the PRC government's use of routers like TP-Link to perpetrate extensive cyberattacks in the United States, it becomes significantly alarming."[87]

91. Cyber threat intelligence researchers with Check Point Research reported in May 2023 that a Chinese state-sponsored hacking group known as Camaro Dragon deployed a malicious firmware implant—containing a custom backdoor named "Horse Shell"—on TP-Link routers, including the TL-WR940N,

---

[86] End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses Before the H. Select Comm. on the Strategic Competition Between the U.S. and the Chinese Communist Party, 119th Cong. (Mar. 5, 2025) (statement of Rob Joyce), https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf.

[87] Rep. John Moolenaar and Rep. Raja Krishnamoorthi, Letter to Department of Commerce Secretary Raimondo (August 13, 2024).

enabling the attackers to maintain persistent access, build anonymous attack infrastructure, and move laterally into compromised networks.[88]

92. TP-Link's Archer router series, along with other models, also has had firmware vulnerabilities reported by the National Institute of Standards and Technology, including a directory traversal vulnerability (CVE-2015-3035) that can allow attackers access to files on the device. The Cybersecurity and Infrastructure Security Agency ("CISA") added that vulnerability to its Known Exploited Vulnerabilities Catalog, confirming it has been exploited in the wild.[89]

93. In April 2025, CISA has cataloged SQL injection vulnerabilities in TP-Link firmware. These vulnerabilities allow "an unauthenticated attacker to inject malicious SQL statements via the username and password fields."[90]

94. Despite TP-Link representing that its networking devices protect consumers' privacy and security, the experts have made the opposite clear. TP-Link's routers have cybersecurity vulnerabilities that hostile state actors have exploited to reach into consumers' homes and businesses. Though these issues have been reported

---

[88] Itay Cohen and Radoslaw Madej, The Dragon Who Sold His Camaro: Analyzing Custom Router Implant, Check Point Research (May 16, 2023), https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/.

[89] National Institute of Standards and Technology, CVE-2015-3035 Detail, National Vulnerability Database, https://nvd.nist.gov/vuln/detail/cve-2015-3035 (last visited Oct. 6, 2026); Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog (CVE-2015-3035 added March 25, 2022), https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[90] Cybersecurity and Infrastructure Security Agency, Vulnerability Summary for the Week of April 14, 2025, https://www.cisa.gov/news-events/bulletins/sb25-111 (last visited Oct. 6, 2026).

on and warned of for years, TP-Link's websites, blogs, and advertisements continue to falsely represent to consumers that its products "protect[] comprehensively."[91] These representations were and are false, deceptive, and material to Florida consumers.

D. TP-Link's Pattern of Critical Cybersecurity Vulnerabilities Continues

95. TP-Link's security failures are not confined to past incidents. Throughout 2026 researchers have continued to disclose critical vulnerabilities across TP-Link's camera, router, and cloud-management product lines.

96. In August 2026, TP-Link disclosed a family of vulnerabilities—CVE-2025-30237 through CVE-2025-30241—affecting its Aginet line of ISP-managed mesh routers, gateways, and modems, which internet service providers distribute directly to homes and small businesses.[92] The lead vulnerability, CVE-2025-30237, is rated high severity (CVSS 8.7) and results from missing authorization checks on internal server endpoints, allowing an unauthenticated attacker with network access to bypass login screens and gain full control of the device.

97. On September 3, 2026, TP-Link published a security advisory disclosing CVE-2026-18167, a high-severity (CVSS 7.7) stack-based buffer overflow in the

---

[91] TP-Link, HomeShield, https://www.tp-link.com/us/homeshield/ (last visited Oct. 6, 2026), archived at https://perma.cc/M8ME-4EX7.

[92] TP-Link, Security Advisory: Multiple Vulnerabilities in ISP-Managed TP-Link Networking Products (CVE-2025-30237 to CVE-2025-30241), https://www.tp-link.com/us/support/faq/5239/ (last visited Oct. 6, 2026), archived at https://perma.cc/ND74-UVZN.

EasyMesh module of its Archer AX55 (v4) router.[93] The Archer AX55 is one of TP-Link's best-selling Wi-Fi 6 routers, and the AX55 has received "Amazon's Choice."[94] An attacker on the router's local network could exploit the flaw to crash the router or, in some circumstances, execute arbitrary code on the device.

98. In late August 2026, TP-Link likewise disclosed CVE-2026-9254, a high-severity (CVSS 8.7) command-injection vulnerability in the parental-control feature of the Archer BE800, Archer BE3600, and Archer AX75 routers.[95] The flaw permits an unauthenticated attacker on the local network to inject commands that execute with root privileges.

99. In September 2026, security researchers at OPSWAT disclosed two vulnerabilities in TP-Link's popular Tapo C120 and C200 smart security cameras. CVE-2026-15315, rated high severity (CVSS 8.7), is an authentication-bypass vulnerability that permits an unauthenticated attacker on the same local network to obtain a valid administrator session without a password, enabling an attacker to alter device settings or view live and recorded video feeds. CVE-2026-15316, also rated high severity (CVSS 7.1), permitted an attacker to crash or restart the camera's security service by sending malformed data. OPSWAT reported both vulnerabilities

---

[93] TP-Link, Security Advisory: Multiple Vulnerabilities in TP-Link Archer AX55 (CVE-2026-18167 & CVE-2026-18330), https://www.tp-link.com/us/support/faq/5279/ (last visited Oct. 6, 2026), archived at https://perma.cc/6K3E-TR26.

[94] https://www.amazon.com/dp/B09G5W9R6R?ref=clp_hp_h_pc&th=1

[95] TP-Link, Security Advisory: Multiple Command Injection Vulnerabilities in Archer Products (CVE-2026-9254, CVE-2026-16348, CVE-2026-78541), https://www.tp-link.com/us/support/faq/5264/ (last visited Oct. 6, 2026), archived at https://perma.cc/2GUR-L82W.

to TP-Link on April 16, 2026; TP-Link did not release a patch until August 18, 2026—more than four months later.[96]

100. In August 2026, researchers with Forescout disclosed fifteen new vulnerabilities in TP-Link's Omada business-networking ecosystem, including CVE-2025-9289.[97] The vulnerabilities stem in part from hard-coded cryptographic keys and predictable device serial numbers in TP-Link's Zero-Touch Provisioning feature, which the researchers found could be exploited to spoof and hijack client devices, inject code into TP-Link's administrative cloud dashboards, and exfiltrate data.

101. These vulnerabilities matter. For example, the ability for a hacker to obtain root-level privileges has real-world privacy and security risks for consumers. It allows a hacker to intercept the raw packet data being transmitted by the consumer through the router (i.e. all of the router traffic), or to redirect traffic and send a consumer to a malicious website.

---

[96] OPSWAT, Authentication Bypass and Denial-of-Service Vulnerabilities: OPSWAT Discovers CVE-2026-15315 & CVE-2026-15316 in TP-Link Tapo Cameras (2026), https://www.opswat.com/blog/authentication-bypass-and-dos-vulnerabilities-opswat-discovers-cve-2026-15315-cve-2026-15316-in-tp-link-tapo-cameras, archived at https://perma.cc/2VTW-YRWU; TP-Link, Security Advisory: Multiple Vulnerabilities in Tapo C120 and C200 (CVE-2026-15315 & CVE-2026-15316), https://www.tp-link.com/us/support/faq/5248/ (last visited Oct. 6, 2026), archived at https://perma.cc/BN9A-84WX.

[97] Forescout, New TP-Link Router Vulnerabilities: Exploiting Zero Touch Provisioning (2026), https://www.forescout.com/blog/new-tp-link-router-vulnerabilities-exploiting-zero-touch-provisioning/, archived at https://perma.cc/CL9F-RLHS; TP-Link, Security Advisory: Response to Research Concerning TP-Link Zero Touch Provisioning (ZTP) Technologies, https://support.omadanetworks.com/us/document/130627/ (last visited Oct. 6, 2026), archived at https://perma.cc/U6UU-T8TE.

V. TP-Link's Data Practices and Privacy Policies Deceive Consumers by Omitting the Risks from China's Intelligence Laws

102. TP-Link's mobile applications collect consumers' personal data and claim to provide customization and control of their privacy and security settings, and its privacy policies reserve broad rights to share that data. But TP-Link fails to disclose a critical fact: TP-Link's Chinese facilities, affiliates, and personnel are subject to PRC national intelligence laws mandating cooperation with PRC intelligence efforts, exposing American consumer data to potential PRC access. By omitting this material fact, TP-Link misleads consumers and fails to obtain informed consent regarding their data within its portfolio of networking and smart home device applications.

103. TP-Link offers applications such as TP-Link Tether, TP-Link Tapo, TP-Link Deco, and Kasa Smart on Apple's App Store and Google's Play Store. These applications can be required to operate TP-Link devices, are integral to the setup and management of TP-Link services such as HomeShield, and grant consumers the ability to customize and control privacy and security settings. These apps are used with a wide range of TP-Link networking and smart home devices, such as cameras, fans, lights, and routers.[98]

104. The Tether Privacy Policy states that TP-Link "may share your personal information internally and externally with suppliers, advisors, or partners for our legitimate business purposes, and only on a need-to-know basis." It carves out the

[98] App Store for iPhone, Kasa Smart, https://apps.apple.com/us/app/kasa-smart/id1034035493 (last visited Oct. 6, 2026).

right to share information with "authorized partners, including affiliates ... to: ... comply with applicable laws," and "where otherwise necessary to protect our rights, interests, and/or property ... or the rights, interests, and/or property of our agents, independent contractors, customers, and others." TP-Link's Deco, Tapo, and Kasa policies contain similar carve-outs.[99]

105. TP-Link's Kasa Smart app points to a "Kasa Privacy Policy (US)" that informs consumers of TP-Link's data collection and use practices. Since at least January 2024, this policy has informed consumers of TP-Link's collection of data, including email, location, and mobile phone identifier. But, under its section titled "How we share personal data," TP-Link states that it "may share information where we have a good faith belief that such disclosure is necessary to (a) comply with an applicable law or legal process."[100] Given TP-Link's deceptive statements about the authority of foreign governments over it, such as "[a]s a company headquartered in the United States, no government—foreign or domestic—has access to and control over the design and production of our routers and other devices,"[101] a consumer would

---

[99] TP-Link, Tether Privacy Policy ¶ 3 (Aug. 20, 2026), https://privacy.tp-link.com/app/Tether/privacy, archived at https://perma.cc/74L4-D2MA; TP-Link, Deco Privacy Policy ¶ 3 (Jan. 5, 2026), https://privacy.tp-link.com/app/Deco/privacy; archived at https://perma.cc/7ZAC-YNF2; TP-Link, Tapo Privacy Policy ¶ 3 (Jan. 23, 2026)), https://privacy.tp-link.com/app/tapo/privacy, archived at https://perma.cc/2WCP-EKEB; TP-Link, Kasa Privacy Policy (US) (Jan. 29, 2024) ¶ 3, https://privacy.tp-link.com/app/kasa/privacy, archived at https://perma.cc/6JQG-QPNZ (each last visited Oct. 6, 2026).

[100] TP-Link, Kasa Privacy Policy (US) (Jan. 29, 2024), https://privacy.tp-link.com/app/kasa/privacy (last visited Oct. 6, 2026).

[101] TP-Link, Fact Sheet, https://www.tp-link.com/us/landing/fact-sheet/ (last visited Oct. 6, 2026), archived at https://perma.cc/9LWY-L3NU.

be deceived by the privacy policy about the risks of the consumers' data being shared with a foreign adversary government.

106. China's 2017 National Intelligence Law compels Chinese organizations and citizens to support, assist, and cooperate with PRC intelligence efforts—a legal obligation DHS has described as compelling PRC entities "to turn over data collected abroad and domestically to the PRC"—backed by penalties including dismissal, investigation, and detention.[102] The U.S. National Security Advisor has separately explained that the National Intelligence Law advances the goals of the PRC's "Military-Civil Fusion (MCF) strategy."[103]

107. TP-Link employs this same omission across its entire suite of applications. The privacy policies are nearly identical on this issue, allowing the collection of personal information such as email, location, and mobile phone identifier while reserving the right to share information to comply with "applicable law or legal process" and to protect the rights of "others."[104] None of these policies discloses that TP-Link's Chinese affiliations subject American consumer data to potential access by

---

[102] U.S. Dep't of Homeland Sec., Data Security Business Advisory 6 (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf; PRC National Intelligence Law (as amended in 2018), China Law Translate (June 27, 2017), https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/ (last visited Oct. 6, 2026).

[103] Statement by National Security Advisor Robert C. O'Brien (Jan. 15, 2021), https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011521-2/.

[104] TP-Link, Tether Privacy Policy (August 20, 2026), https://privacy.tp-link.com/app/Tether/privacy; TP-Link, Deco Privacy Policy (January 5, 2026), https://privacy.tp-link.com/app/Deco/privacy; TP-Link, Tapo Privacy Policy (January 23, 2026)), https://privacy.tp-link.com/app/tapo/privacy (each last visited Oct. 6, 2026).

PRC intelligence agencies. And TP-Link makes deceptive statements about the authority of foreign governments over it. When TP-Link reserves the right to share data to "comply with applicable laws" or protect the rights of "others," there is a specific China-related risk lurking behind those words that would be material to many consumers, but TP-Link deceptively omits such risk.

VI. Federal and State Authorities Have Recognized the Risks Posed by TP-Link Devices

108. In December 2024, it was publicly reported that the U.S. Departments of Commerce, Defense, and Justice had opened investigations into TP-Link concerning national security risks posed by its routers.[105]

109. In October 2025, it was reported that federal officials had concluded that TP-Link's ties to China may pose an "unacceptable risk" and were weighing a proposed plan to ban the sale of TP-Link routers in the United States.[106]

110. On March 23, 2026, the FCC's Public Safety and Homeland Security Bureau announced the addition of routers produced in foreign countries to the FCC's Covered List, explaining that "[r]outers are the key networking device that enable American homes, schools, businesses, critical infrastructure providers, and emergency services to connect to the internet every day," and that "[c]ompromised

[105] Heather Somerville, Dustin Volz & Aruna Viswanatha, *U.S. Weighs Ban on China-Made TP-Link Routers*, Wall St. J. (Dec. 18, 2024).

[106] Kate O'Keeffe, Josh Sisco & Kate Sullivan, *US Weighs Action Against China-Linked Router Giant TP-Link*, Bloomberg (Oct. 9, 2025).

routers can enable in-depth network surveillance, data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses' networks."[107]

111. It has since been reported that TP-Link is seeking conditional approval from the FCC to sell new router models in the United States.[108]

112. In June 2026, the Department of Defense's designations under Section 1260H identified TP-Link Technologies as a Chinese military company, alongside Hikvision and Dahua, whose devices were compromised in the same Quad7 botnet as TP-Link's routers.[109]

---

[107] FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List, WC Docket No. 18-89, Public Notice, DA 26-278, App. C at 1 (Mar. 23, 2026), https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf.

[108] Michael Kan, *Facing Router Ban, TP-Link Tells FCC It's Investing Hundreds of Millions in the US*, PCMag (Apr. 23, 2026), https://www.pcmag.com/news/facing-router-ban-tp-link-tells-fcc-its-investing-hundreds-of-millions.

[109] Gi7w0rm, *The Curious Case of the 7777 Botnet*, Medium (Oct. 19, 2023), https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd, archived at https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd; Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35192–94 (June 10, 2026) (designating Hangzhou Hikvision Digital Technology Co., Ltd., TP-Link Technologies Co., Ltd., and Zhejiang Dahua Technology Co., Ltd.); U.S. Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (June 8, 2026), https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF.

VII. TP-Link's Conduct Harms Florida Consumers, Including Senior Citizens, Servicemembers, and Persons with Disabilities

113. Florida consumers have purchased, and continue to purchase, TP-Link routers, networking devices, smart home devices, and related applications and services in reliance on TP-Link's representations regarding security, privacy, and supply-chain integrity. Consumers keep routers in service for years, meaning that deceptively marketed and no-longer-supported TP-Link devices remain in Florida homes and small businesses today.

114. On information and belief, the Florida consumers victimized by Defendant's conduct include senior citizens aged 60 or older, persons with disabilities, military servicemembers and their spouses and dependent children, and veterans, within the meaning of Section 501.2077, Florida Statutes. Florida is home to one of the largest populations of senior citizens, servicemembers, and veterans in the United States, and, on information and belief, members of each group purchased and continue to use TP-Link devices in their homes.

115. Defendant knew or should have known that its acts and practices described in this Complaint were unfair, deceptive, or unconscionable. Defendant's violations of FDUTPA were therefore willful within the meaning of Sections 501.2075 and 501.2077, Florida Statutes.

COUNT I
DECEPTIVE ACTS OR PRACTICES IN VIOLATION OF FDUTPA: FALSE AND DECEPTIVE SECURITY REPRESENTATIONS (§ 501.204(1), Fla. Stat.)

116. The Attorney General adopts, incorporates, and realleges paragraphs 1-115 as if fully set forth here.

117. Section 501.204(1), Florida Statutes, declares unlawful "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce."

118. A deceptive act or practice is one that is likely to mislead consumers acting reasonably in the circumstances, to the consumers' detriment.

119. Defendant engaged in deceptive acts or practices in the conduct of trade or commerce, in violation of Section 501.204(1), Florida Statutes, by, without limitation:

a. Representing, expressly and by implication, that TP-Link devices are secure—including that HomeShield "covers all security scenarios," "handles all your concerns," and provides "preventions against any potential cyber threats or attacks," and formerly that HomeShield provides a "100% safeguard"—despite security flaws and vulnerabilities;

b. Making model-specific security representations—including that the TL-WR940N provides "[e]asy wireless security encryption" and "access control"; that the Archer C7 "provides secure Wi-Fi access for guests"; that the Archer AX21 offers "Refined Password Security" and a "New Level of Cyber Security"; and that the Archer AXE75 has "advanced security features that deliver a safe environment"—when those models contained critical, actively exploited vulnerabilities;

c. Making false or deceptive statements after vulnerabilities became public, including TP-Link's April 2026 representation that all products

affected by the Quad7 attacks had reached end-of-life status, which omitted the TL-WR940N until TP-Link corrected the omission in May 2026; and

d. Selling devices to Florida consumers while failing to disclose material facts about repeated critical security vulnerabilities—including vulnerabilities exploited by Chinese state-sponsored hackers and the Russian GRU—and about default settings that do not support automatic firmware updates, leaving consumers unknowingly exposed.

120. Defendant's violations are continuing. Each deceptive representation, omission, sale, offer for sale, and advertisement constitutes a separate and independent violation of FDUTPA for which civil penalties may be imposed. §§ 501.2075, 501.2077, Fla. Stat.

COUNT II
DECEPTIVE ACTS OR PRACTICES IN VIOLATION OF FDUTPA: CORPORATE SEPARATION, SUPPLY-CHAIN, AND MANUFACTURING REPRESENTATIONS AND OMISSIONS
(§ 501.204(1), Fla. Stat.)

121. The Attorney General adopts, incorporates, and realleges paragraphs 1-115 as if fully set forth here.

122. Defendant engaged in deceptive acts or practices in the conduct of trade or commerce, in violation of Section 501.204(1), Florida Statutes, by, without limitation:

a. Representing that TP-Link completely separated from its Chinese operations—including that the corporate split "encompass[ed] all

shareholdings and operational aspects, including legal entities, workforce, research and development, production, marketing, and customer service," and that "no government—foreign or domestic—has access to and control over the design and production of our routers and other devices"—when much of TP-Link's research, development, and manufacturing remains in China, entrenched in China's state-sponsored technology ecosystem;

b. Representing that TP-Link manufactures its products for the U.S. market in its own Vietnamese facility and that such manufacturing "provides another layer of security and governance for the supply chain," when only 0.5% of the components by value are bought in Vietnam, all other inputs are imported from or through China, and a U.S.-designated Chinese military company performed recent construction at the facility;

c. Omitting material facts about TP-Link's ongoing reliance on Chinese manufacturing, research and development, subsidies, suppliers, and affiliates, including the June 2026 designation of TP-Link Technologies as a Chinese military company operating in the United States; and

d. Omitting material facts about the Chinese legal regime—including the 2017 National Intelligence Law and the 2021 Regulations on the Management of Security Vulnerabilities in Network Products (RMSV)—applicable to TP-Link's Chinese facilities, affiliates, and personnel.

123. Defendant's violations are continuing. Each deceptive representation, omission, sale, offer for sale, and advertisement constitutes a separate and

independent violation of FDUTPA for which civil penalties may be imposed. §§ 501.2075, 501.2077, Fla. Stat.

COUNT III
DECEPTIVE ACTS OR PRACTICES IN VIOLATION OF FDUTPA: DATA-PRACTICES OMISSIONS
(§ 501.204(1), Fla. Stat.)

124. The Attorney General adopts, incorporates, and realleges paragraphs 1-115 as if fully set forth here.

125. Defendant engaged in deceptive acts or practices in the conduct of trade or commerce, in violation of Section 501.204(1), Florida Statutes, by, without limitation:

a. Collecting Florida consumers' personal data—including email addresses, precise location, and mobile phone identifiers—through its Tether, Deco, Tapo, and Kasa Smart applications, while reserving broad rights to share that data with "affiliates" to "comply with applicable laws" and to protect the rights of "others," without disclosing that Defendant's Chinese facilities, affiliates, and personnel are subject to PRC national intelligence laws that expose collected or shared data to potential access by PRC intelligence agencies under PRC law; and

b. Representing that its applications provide consumers with customization and control over their privacy and security settings while omitting the same material facts, thereby depriving consumers of the ability to give informed consent to Defendant's collection, use, and sharing of their personal data.

126. Defendant's omissions were material to Florida consumers and rendered its affirmative representations—including that "no government—foreign or domestic—has access to and control over the design and production" of its devices—misleading. Defendant's violations are continuing. Each such omission, representation, offer for sale, advertisement, and sale constitutes a separate and independent violation of FDUTPA for which civil penalties may be imposed. §§ 501.2075, 501.2077, Fla. Stat.

COUNT IV
UNFAIR ACTS OR PRACTICES IN VIOLATION OF FDUTPA
(§ 501.204(1), Fla. Stat.)

127. The Attorney General adopts, incorporates here, and realleges paragraphs 1-115 as if fully set forth here.

128. An unfair practice under FDUTPA is one that offends established public policy, or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. A practice is also unfair where it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or to competition. § 501.204(2), Fla. Stat.; *see also* 15 U.S.C. § 45(n).

129. Defendant engaged in unfair acts or practices in the conduct of trade or commerce, in violation of Section 501.204(1), Florida Statutes, by, without limitation:

a. Continuing to market and sell TP-Link devices in Florida as secure despite knowledge that its devices have been exploited in state-sponsored

cyberattack campaigns, including by Chinese threat actors and the Russian GRU, against American consumers, businesses, and critical infrastructure;

b. Ceasing security support for router models—including the TL-WR940N, Archer C7 (v2 and v3), and Archer AX21 (v1 and v1.20)—that TP-Link knows remain in consumers' homes, that do not support automatic firmware updates, and that contain known, actively exploited vulnerabilities; and

c. Shipping routers with default settings that do not support automatic firmware updates, so that protection against known, actively exploited vulnerabilities requires consumers to learn of the vulnerability and manually locate, download, and install firmware patches.

130. These practices cause and are likely to cause substantial injury to Florida consumers—including the conscription of consumers' routers into foreign state-sponsored botnets and the exposure of their communications and personal data—that consumers cannot reasonably avoid, because firmware vulnerabilities, Chinese supply-chain dependencies, and foreign legal obligations are not discoverable by ordinary consumers, and that is not outweighed by any countervailing benefit to consumers or competition.

131. Each unfair act or practice constitutes a separate and independent violation of FDUTPA. §§ 501.2075, 501.2077, Fla. Stat.

COUNT V
UNCONSCIONABLE ACTS OR PRACTICES IN VIOLATION OF FDUTPA
(§ 501.204(1), Fla. Stat.)

132. The Attorney General adopts, incorporates here, and realleges paragraphs 1-115 as if fully set forth here.

133. Section 501.204(1), Florida Statutes, prohibits unconscionable acts or practices in the conduct of any trade or commerce.

134. Defendant engaged in unconscionable acts and practices in the conduct of trade or commerce, in violation of Section 501.204(1), Florida Statutes, by, without limitation:

a. Continuing to market and sell certain TP-Link devices in Florida as secure despite knowledge that its devices have been exploited in state-sponsored cyberattack campaigns against American consumers, businesses, and critical infrastructure;

b. Exploiting consumer trust by marketing its devices as the secure guardian of consumers' home networks while aware of ongoing, repeated, and critical vulnerabilities;

c. Ceasing security support for router models that TP-Link knows remain in consumers' homes, that do not support automatic firmware updates, and that contain known, actively exploited vulnerabilities;

d. Failing to disclose that TP-Link devices are dependent on Chinese components, facilities, and affiliates subject to PRC laws mandating

cooperation with PRC intelligence services and two-day disclosure of security vulnerabilities to the Chinese government;

e. Marketing and selling TP-Link products while aware of federal investigations and governmental designations concerning the national security risks of its devices, and failing to disclose those facts to consumers; and

f. Using vague privacy policies and manufacturing representations that shift responsibility to consumers while affirmatively creating the false impression that its products are safe, secure, and unaffiliated with China.

135. Defendant's acts and practices are procedurally unconscionable. Florida consumers had no meaningful ability to discover the concealed facts or to protect themselves: firmware vulnerabilities cannot be detected by ordinary inspection; supply-chain dependencies and foreign legal obligations were known only to Defendant; Defendant's device terms, application privacy policies, and end-of-life policy are presented on a take-it-or-leave-it basis with no opportunity to negotiate; and TP-Link's dominance of the United States retail router market limited consumers' practical alternatives.

136. Defendant's acts and practices are also substantively unconscionable. The resulting bargains were unreasonably one-sided in Defendant's favor, leaving Florida consumers with devices that were insecure, that would lose security support at Defendant's election, and that were subject to undisclosed foreign legal obligations, while Defendant retained the full purchase price.

137. Each unconscionable act or practice constitutes a separate and independent violation of FDUTPA. §§ 501.2075, 501.2077, Fla. Stat.

TRIAL BY JURY

138. Plaintiff demands a trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, the Office of the Attorney General, State of Florida, Department of Legal Affairs, respectfully requests that this Court:

A. Enter Judgment for the Attorney General and against the Defendant for violations of the Florida Deceptive and Unfair Trade Practices Act, Section 501.204(1), Florida Statutes;

B. Permanently enjoin Defendant, its officers, directors, agents, servants, employees, successors, assigns, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in the deceptive, unfair, and unconscionable acts and practices alleged here, pursuant to Section 501.207(1)(b), Florida Statutes;

C. Order Defendant to disgorge all ill-gotten gains, money, or property acquired by means of those violations, pursuant to Section 501.207, Florida Statutes, and the Court's equitable powers;

D. Assess against Defendant civil penalties of $10,000 for each willful violation of FDUTPA, pursuant to Section 501.2075, Florida Statutes, and $15,000 for each willful violation victimizing, or attempting to victimize, a senior citizen, a person who has a disability,

or a willful violation directed at a military servicemember, the spouse or dependent child of a military servicemember, or a veteran, pursuant to Section 501.2077, Florida Statutes;

E. Award Plaintiff its reasonable attorney's fees and costs, under Sections 501.2075 and 501.2105, Florida Statutes; and

F. Grant such other and further relief as this Court deems just and proper.

Date: October 6, 2026.

Respectfully Submitted,

JAMES UTHMEIER
Attorney General

RYAN D. NEWMAN
Chief Deputy Attorney General

JASON HILBORN
Deputy Attorney General
Civil Division

Brunn (Beau) Roysden*
Brett Talley*
CULPER LAW PLLC
111 W. Marshall Ave.
Phoenix, Arizona 85013
Telephone: 602-315-7545
beau@culper.law
brett@culper.law

**Pro hac vice forthcoming*

/s/ Henry Q. Johnson
Henry Q. Johnson (FBN 144274)
Senior Assistant Attorney General
FLORIDA OFFICE OF THE ATTORNEY GENERAL
110 SE 6th Street, 10th Floor
Fort Lauderdale, FL 33301
Telephone: (954) 712-4600
Henry.Johnson@myfloridalegal.com

Cristina Hernandez Villar (FBN 102305)
Senior Assistant Attorney General
FLORIDA OFFICE OF THE ATTORNEY GENERAL
110 SE 6th Street, 10th Floor
Fort Lauderdale, FL 33301
Telephone: (954) 712-4600
Cristina.HernandezVillar@myfloridalegal.com

Diane K. Oates (FBN 116233)
Chief, Assistant Attorney General
FLORIDA OFFICE OF THE ATTORNEY GENERAL
1 S.E. Third Avenue, Suite 900
Miami, Florida 33131
Telephone: (305) 377-5835
Diane.Oates@myfloridalegal.com