CAUSE NO: _____

THE STATE OF TEXAS	**§**	**IN THE DISTRICT COURT**
	§	
Plaintiff,	**§**	
v.	**§**	
	§	**COLLIN COUNTY, TEXAS**
TP-LINK SYSTEMS INC.	**§**	
	§	
Defendant.	**§**	
	§	
	§	
	§	
	§	**_____JUDICIAL DISTRICT**

TEXAS'S ORIGINAL PETITION AND APPLICATION FOR TEMPORARY AND PERMANENT INJUNCTIONS

In an era where life is increasingly digital, a family's router serves as the digital front door to their private lives. Millions of families trust TP-Link to guard that door. They do so based on TP Link's repeated assurances that it is a company distinct from the geopolitical risks posed by China. But these families are unaware that the same TP-Link devices meant to protect them are actually exposing them.

Behind TP-Link's "Made in Vietnam" stickers is a supply chain deeply entrenched in China, where nearly all of TP Link's components are sourced before being shipped to Vietnam for mere final assembly. TP-Link has created a web of deception that includes shared manufacturing, research, and Chinese state-sponsored benefits, with the company's leadership acknowledging accolades and subsidies from the Chinese government. By masking its Chinese connections, TP-Link has exposed millions of consumers to severe cybersecurity risks, including firmware vulnerabilities exploited by Chinese hacking groups. Instead of the secure doorway consumers

expect, TP-Link devices are an open window for Chinese-sponsored threat actors and Chinese intelligence agencies.

Realizing this grave threat to Texas consumes, on January 26, 2026, Governor Greg Abbott, in consultation with Texas Cyber Command, updated Texas' Prohibited Technologies List to include TP-Link.[1] The list of prohibited technologies is made, in part, to "protect the privacy of Texans from the People's Republic of China" and "the Chinese Communist Party." A company's inclusion on the prohibit technologies list prohibits the use of that company's hardware on state-owned devices and networks.[2]

TP-Link's deception violates Texas law and must stop now. The Texas Deceptive Trade Practices Act prevents Big Tech companies like TP-Link from selling Texans devices through these types of false, misleading, and deceptive trade practices. TP-Link devices are currently for sale at major retailers throughout the State of Texas, hiding vulnerabilities behind misrepresentations of its affiliation and protection. Meanwhile, other TP-Link devices are already connected inside of Texas homes and businesses, lying in wait. TP-Link's devices are not the secure American devices that Texas consumers have consented to purchase. They are modern weapons of war, enabling a foreign adversary to surveil and attack the United States. The State of Texas brings this suit to end this deceptive scheme, protect Texans' privacy, and hold TP-Link accountable for trading safety and security for market dominance.

[1] *See* https://gov.texas.gov/news/post/governor-abbott-updates-texas-prohibited-technologies-list.
[2] *See* https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies.

Texas Attorney General Ken Paxton, on behalf of the State of Texas, hereby sues Defendant TP-Link Systems Inc. ("TP-Link") for violations Tex. Bus & Com. Code § 17.46 (the Texas Deceptive Trade Practices Act or "DTPA"), and Chapter 521 of the Texas Business and Commerce Code.

I. PARTIES

1. The Plaintiff, the State of Texas, by and through Ken Paxton, Attorney General, is charged with enforcing the DTPA. Pursuant to TEX. BUS. & COM. CODE ANN. § 17.47, the Attorney General may initiate civil law enforcement proceedings in the name of the State to enjoin violations of the DTPA and to obtain other relief as may be appropriate in each case.

2. Defendant, TP-Link Systems Inc. ("TP-Link") is a foreign corporation regularly transacting, soliciting, and conducting business in Texas, that has its U.S. based headquarters in Irvine, California.

II. JURISDICTION AND VENUE

3. This action is brought by the Texas Attorney General's Office through its Consumer Protection Division in the name of the State of Texas ("Plaintiff" or the "State") and in the public interest, pursuant to the authority granted by Section 17.47 of the Texas Deceptive Trade Practices Act ("DTPA").

4. Venue is proper in Collin County, Texas, because a substantial part of the events or omission giving rise to Texas's claims occurred in Collin County, because TP-Link has done business with retailers and consumers in Collin County, because TP-Link unlawfully surveilled consumers who own TP-Link devices in Collin County, and because TP-Link advertised and sold

networking and smart home devices to consumers at locations in Collin County, including but not limited to those sold at Best Buy located at 190 E Stacy Rd Bldg 3000, Allen, TX 75002; Best Buy located at 1751 N Central Expy Ste C, McKinney, TX 75070; and at Walmart Supercenter, 5001 McKinney Ranch Pkwy, McKinney, TX 75070. *See* Tex. Bus. & Com. Code §§ 17.47(b).

5. Texas courts may exercise personal jurisdiction over a nonresident entity if the Texas long-arm statute authorizes the exercise of personal jurisdiction and the exercise is consistent with federal, and state constitutional due-process guarantees. *State v. Yelp, Inc.*, 725 S.W.3d 170, 181-187 (Tex. App.—15th Dist. 2025, pet. filed), *Moki Mac Rivr Expeditions v. Drugg*, 221 S.W.3d 569, 574 (Tex. 2007); *see also* Tex. Civ. Prac. & Rem. Code § 17.042 (Texas long-arm statute).

6. Jurisdiction is proper because TP-Link has established minimum contacts in Texas such that maintenance of this suit does not offend traditional notions of fair play and substantial justice, *see Int'l Shoe Co. v. State of Wash., Off. of Unemployment Comp. & Placement*, 326 U.S. 310, 316 (1945), and because TP-Link transacts business in Texas and is therefore subject to Texas' long-arm statute, *see* Tex. Civ. Prac. & Rem. Code §§ 17.001–093.

7. The Court has general jurisdiction over TP-Link because its contacts and affiliations with Texas are so continuous and systematic as to render them essentially at home in Texas. *BMC Software Belg., N.V. v. Marchand*, 83 S.W.3d 789, 797 (Tex. 2002).

8. TP-Link has failed to register with the Secretary of State as required under Chapter 9 of the Texas Business Organizations Code. Tex. Bus. Orgs. Code § 9.001(a). In the event TP-Link comes into compliance and registers, the Court has jurisdiction over TP-Link because it

consented to personal jurisdiction by registering and transacting business in Texas. *See Mallory v. Norfolk S. Ry. Co.*, 600 U.S. 122 (2023); *see also Acacia Pipeline Corp. v. Champlin Expl., Inc.*, 769 S.W.2d 719, 720 (Tex. App.—Houston [1st Dist.] 1989, no writ) ("In return for the privilege of doing business in Texas, and enjoying the same rights and privileges as a domestic corporation, Champlin has consented to amenability to jurisdiction for purposes of all lawsuits within the state.").

9. Alternatively, the Court has specific jurisdiction over TP-Link because it purposefully availed itself of the privileges of conducting activities in Texas and the causes of action in this suit arise out of or relate to TP-Link's contacts in Texas, including the advertising and sale of millions of networking and smart home devices in Texas and the unlawful Chinese surveillance and cyberthreats towards millions of consumers in Texas. *Luciano v. SprayFoamPolymers.com, LLC*, 625 S.W.3d 1, 9 (Tex. 2021).

III. DISCOVERY CONTROL PLAN

10. Discovery in this case should be conducted under Level 3 pursuant to Texas Rule of Civil Procedure 190.4. Restrictions concerning expedited discovery under Texas Rule of Civil Procedure 169 do not apply because Texas seeks non-monetary injunctive relief as part of its claims.

11. Additionally, Texas claims entitlement to monetary relief in an amount greater than $1,000,000.00, including civil penalties, reasonable attorneys' fees, litigation expenses, and costs.

IV. PUBLIC INTEREST

12. The Consumer Protection Division has reason to believe that TP-Link is engaging in, has engaged in, or is about to engage in an act or practice declared to be unlawful under the DTPA and that proceedings would be in the public interest to restrain by permanent injunction the use of such method, act, or practice. Tex. Bus. & Com. Code § 17.47(a).

13. The public interest in this enforcement action is underscored by Governor Greg Abbott's designation of TP-Link as a prohibited technology under Texas' Prohibited Technologies List to protect Texans' privacy from the People's Republic of China and the Chinese Communist Party.

V. TRADE AND COMMERCE

14. At all times described below, TP-Link and its agents have engaged in conduct which constitutes "trade" and "commerce" defined in § 17.45(6) of the DTPA.

15. At all times described below, TP-Link and its agents engaged in transactions with Texans who are considered "consumers" within the meaning of § 17.45(4) of the DTPA.

VI. FACTUAL ALLEGATIONS

16. TP-Link is a global provider of networking and smart home devices for consumers and small to mid-size organizations. Founded in 1996 by brothers Zhao Jiaxing ("Cliff Chao") and Zhao Jianjun ("Jeffrey Chao") in Shenzhen, China, TP-Link expanded into the United States market in 2008 by establishing TP-Link USA. By 2016, TP-Link USA reported revenues exceeding $2 billion.

3

17. After more than a decade of success in the United States 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 operations through the entity TP-LINK Technologies Co., Ltd., and Jeffrey Chao became the CEO and owner of Defendant TP-Link Systems Inc.[4] TP-Link represented that this divide "encompass[ed] all shareholdings and operational aspects, including legal entities, workforce, research and development, production, marketing, and customer service."[5] In March of 2025, TP-Link again represented that it had "entirely different ownership, management, and operations" than TP-LINK Technologies Co. Ltd.[6]

[3] *Tom's Hardware, TP-Link Archer BE3600 Wi-Fi 7 router review: Dual-band Wi-Fi 7 for less than $100*, https://www.tomshardware.com/networking/routers/tp-link-archer-be3600-wi-fi-7-router-review (Photograph of TP-Link Archer BE3600 router) (last accessed February 13, 2026).

[4] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinge on Its Claimed Split From China*, Bloomberg (April 11, 2025).

[5] TP-Link, TP-Link Group TP-Link Corporation Group Announces Completion of Corporate Restructuring, Marking a New Era in its Future Evolution (May 11, 2024).

[6] *TP-Link*, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (March 5, 2025).

18. TP-Link represents to American consumers that the devices it markets and sells in the United States are made in Vietnam. 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.[7] Consistent with that representation, for years TP-Link devices in the American market have included a "Made in Vietnam" sticker to signal this to consumers.

19. TP-Link is the dominant player in the United States' networking and smart home technology market. TP-Link controls 65% of the United States' market for networking devices.[8] TP-Link's smart-phone applications are ranked as the top downloads in Apple's App Store's "Utilities" category. And TP-Link's sponsored Amazon listings show tens of thousands of monthly purchases.

I. TP-Link's False, Deceptive and Misleading Representations Regarding its Chinese Supply Chain

20. TP-Link's express and implicit representations that its networking and smart home devices' have no of ties to China are false, misleading, and deceptive. TP-Link and Jeffrey Chao own and manage Chinese subsidiaries and facilities that manufacture, research, and develop TP-Link's networking and smart home devices. TP-Link's operations rely on China and TP-Link Technologies. And despite TP-Link's "Made in Vietnam" stickers, nearly all of the components found inside of TP-Link's devices are imported from China. TP-Link's mere last-step assembly in Vietnam does not cure the company's deceit of Chinese origin and affiliation.

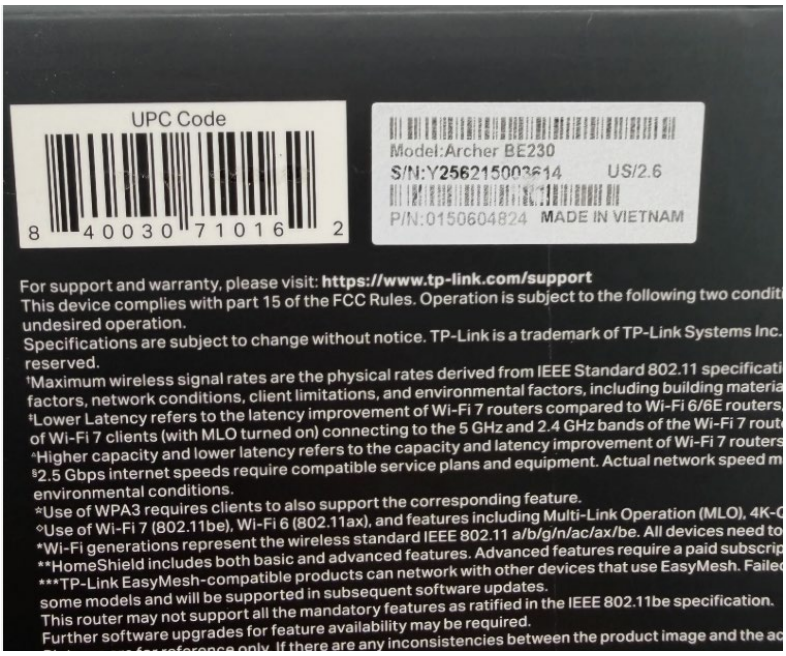
[7] *TP-Link*, BFG Group Announcement (September 19, 2023).
[8] *End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party*, 119th Cong. (2025), (statement of Rob Joyce).

21. Since 2018, TP-Link has represented that its products sold in the United States are manufactured in Vietnam.[9] In 2025, after the House Select Committee on the Chinese Communist Party held a meeting discussing TP-Link's relation to Chinese state-sponsored cyberattacks, TP-Link represented it "manufactures [its] own routers in Vietnam in [its] own facility."[10] On information and belief, TP-Link's device packaging has used a "Made in Vietnam" sticker at retailers across Texas since at least 2020.

22. The reality behind TP-Link's Vietnamese manufacturing claims tells a different story. According to TP-Link itself, it "still has substantial operations in mainland China."[11] The numbers bear that out, components sourced from Vietnam account for less than 1 percent of the components used to assemble devices in TP-Link's Vietnamese factory; the vast majority are imported from China.[12] TP-Link has operational control over at least four major facilities in China to manufacture routers.[13] These facilities include TP-Link's Shenzhen Research and Development Center, Shenzhen Manufacturing Center, Dongguan Manufacturing Center, and Shenzhen Guangqiao Manufacturing Center.[14] Further, TP-Link is building a fifth engineering facility in Chengdu, China.[15]

---

[9] Pl.'s Ex. A.
[10] *TP-Link*, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (March 5, 2025).
[11] Kate O'Keeffe, Josh Sisco, and Kate Sullivan, *US Weighs Action Against China-Linked Router Giant TP-Link*, Bloomberg Law (October 9, 2025).
[12] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinge on Its Claimed Split From China*, Bloomberg (April 11, 2025).
[13] TP-Link, 2024 Sustainability Report, (last accessed February 13, 2026), https://static-page.tp-link.com/sustainability/pdf/TP-Link%202024%20Sustainability%20Report.pdf.
[14] *Id.*
[15] *Id.*



16

23. Jeffrey Chao has previously acknowledged that TP-Link's Chinese facilities and subsidiaries have "recently received state accolades and benefits."[17] The Chinese government utilizes subsidies, such as lucrative tax breaks, free land, and expedited permitting for industrial facilities, to compete against the United States.[18] That relationship runs deeper than financial support. Hunan, a Chinese province, recently announced that TP-Link's Vietnamese factory was

[16] eBay, TP-Link Archer BE230 BE3600 Dual-Band WiFi 7 Router 2.5Gbps 9K, https://ebay.us/m/yEmudu, (last accessed February 13, 2026).
[17] Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinge on Its Claimed Split From China*, Bloomberg (April 11, 2025).
[18] 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 accessed February 13, 2026).

one of its "Key Projects for Foreign Investment and Corporation."[19] The notice reportedly stated that a Chinese military company was working to expand TP-Link's manufacturing, research, and development facilities in Vietnam.[20]

24. Reporting and trade data confirms that TP-Link has imported its devices into the United States from China for years. TP-Link's shipments from Lianzhou Technologies Co., Ltd have departed from Shanghai, China to Long Beach California, as recently as January of 2026.[21] Lianzhou Technologies Co., Ltd. is the entity responsible for TP-Link's Shenzhen Research and Development Center.[22] In fact, TP-Link Systems Inc. has imported over 49 shipments of networking and smart home devices from its Chinese-affiliated companies, such as TP-LINK Technologies and Lianzhou Technologies Co., Ltd.[23]

25. On information and belief, TP-Link also utilizes TP-Link USA Corp. to import from China. According to trade information, TP-Link USA Corp. has had shipments from Shanghai, China as recently as December of 2025.[24] This further shows that TP Link's connection to China regardless of the corporate entity used to receive the goods.

---

[19] 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, (last accessed on February 13, 2026).

[20] *Id.*

[21] ImportGenius, *Lianzhou Technologies Co., Ltd*, https://www.importgenius.com/suppliers/lianzhou-technologies-co-ltd, (last accessed on February 13, 2026).

[22] TP-Link, 2024 Sustainability Report, (last accessed February 13, 2026), https://static-page.tp-link.com/sustainability/pdf/TP-Link%202024%20Sustainability%20Report.pdf.

[23] ImportInfo, TP-LINK SYSTEMS INC, https://www.importinfo.com/tp-link-systems-inc, (last accessed February 13, 2026).

[24] ImportInfo, TP-LINK USA CORPORATION, https://www.importinfo.com/tp-link-usa-corporation, (last accessed February 13, 2026).

26. TP-Link omits material facts to deceive consumers into thinking it's Vietnamese-assembled products are unaffiliated with China. The reality is that TP-Link continues to operate its supply-chain deep inside of China, with China's support, and through Chinese exports. The final touches TP-Link makes in Vietnam do not cure the company's deceit of its Chinese affiliations.

II. TP-Link's False, Deceptive, and Misleading Representations About the Privacy and Security of its Networking Devices

27. TP-Link represents to consumers that its networking devices protect their privacy and security. As detailed below, that representation is false, these devices are not secure. Security experts and researchers have reported on TP-Link's numerous and dangerous firmware vulnerabilities for years, as Chinese state-sponsored hackers exploited these vulnerabilities to access American consumers' networks, data, and devices. Despite these faults, TP-Link's websites, blogs, and advertisements continue to insist its products maintain consumers' privacy and security in totality.

28. TP-Link represents that its routers, such as the Archer BE9700 Router sold at Best Buy in Allen and McKinney, feature "Network Security with Homeshield."[25] Homeshield is a "built-in service" that provides consumers with privacy and security controls over their homes' and businesses' networks. TP-Link makes numerous representations to consumers regarding Homeshield privacy and security capabilities in order to induce them into buying. TP-Link

[25] BestBuy, TP-Link – Archer BE9700 Tri-Brand Wi-Fi Router – Black, https://www.bestbuy.com/product/tp-link-archer-be9700-tri-band-wi-fi-7-router-black/J39T6X26PS, (last accessed on February 13, 2026).

represents that Homeshield "covers all security scenarios,"[26] that it provides a "100% safeguard" for network security,"[27] that it handles all concerns regarding "cyber virus intrusions" and "IoT device attacks,"[28] and that it "protect[s] all your IoT and other connected devices from any cyber threats and attacks."[29] Consumers trust TP-Link's representations when considering which device they are to purchase. TP-Link knows this, and TP-Link knows of its devices' plethora of vulnerabilities.

29. 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.[30] Former Director of the Cybersecurity the National Security Agency Rob Joyce has testified that "TP-Link routers were among the various brands exploited by Chinese State Sponsored hackers in the massive Volt, Flax, and Salt typhoon attacks."[31]

30. Chairman of the United States House of Representative's 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

---

[26] TP-Link, Homeshield, https://www.tp-link.com/us/homeshield/, (last accessed on February 13, 2026).
[27] Pl.'s Ex. B.
[28] TP-Link, Homeshield, https://www.tp-link.com/us/homeshield/, (last accessed on February 13, 2026).
[29] *Id.*
[30] 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, (last accessed February 13, 2026).
[31] *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).

investigation.[32] "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."[33]

31. Cyber threat intelligence researchers with Check Point Research reported that hacking campaigns from Camaro Dragon, a Chinese state-sponsored hacking group, were made possible through firmware vulnerabilities in TP-Link routers.[34]

32. Poor security in TP-Link's AC1200 Archer router made it possible for hackers to gain network privileges, leak credentials, and steal data; techniques that allow for far longer and more invasive snooping and malign control.[35]

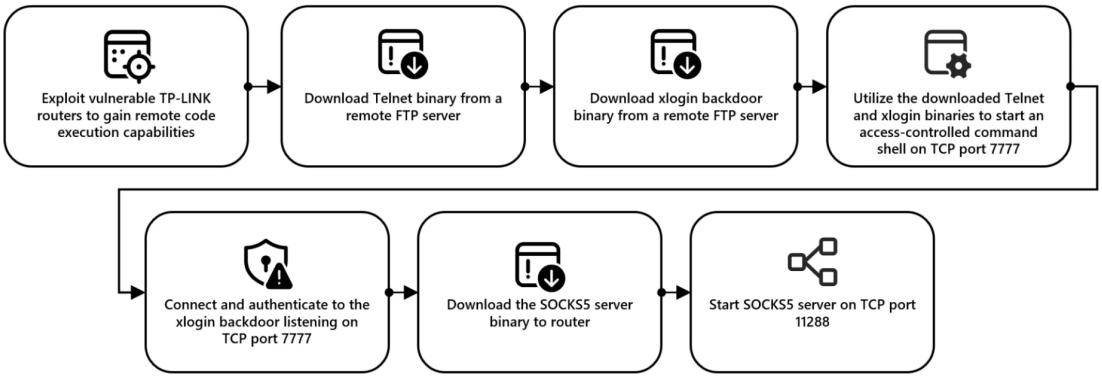
33. TP-Link's Archer router series, along with other models, also have reported firmware vulnerabilities by the National Institute of Standards and Technology.[36] Here, the report details a directory transversal vulnerability, which can allow attackers access to files.[37]

---

[32] Rep. John Moolenaar and Rep. Raja Krishnamoorthi, *Letter to Department of Commerce Secretary Raimondo,* (August 13, 2024).
[33] *Id.*
[34] 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/, (last accessed February 13, 2026).
[35] Rebecca Grant, *Bye Bye Bad Chinese Routers*, Real Clear Defense (May 21, 2024), https://www.realcleardefense.com/2024/05/31/bye_bye_bad_chinese_routers_1035006.html, (last accessed February 13, 2026).
[36] National Institute of Standards and Technology, *CVE-2015-3035 Detail*, National Vulnerability Database, https://nvd.nist.gov/vuln/detail/cve-2015-3035, (last accessed February 13, 2026)
[37] Cybersecurity and Infrastructure Security Agency, *Known Exploited Vulnerabilities Catalog*, https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=tp

34. In October of 2024, Microsoft reported that a Chinese threat actor known as Storm-940 was utilizing compromised TP-Link routers to conduct "password spraying."[38] Password spraying is when a hacker gains unauthorized access to information by utilizing a single password on several accounts at once.

35. In April of 2025, the Cybersecurity and Infrastructure Security Agency ("CISA") issued notice that an SQL injection vulnerability in TP-Link's firmware had been discovered.[39] This vulnerability allows "an unauthenticated attacker to inject malicious SQL statements visa the username and password fields."[40]



link&field_date_added_wrapper=all&sort_by=field_date_added&items_per_page=20 (Search page results after searching for TP-Link) (last accessed February 13, 2026).

[38] 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/, (last accessed February 13, 2026).

[39] Cybersecurity and Infrastructure Security Agency, *Vulnerability Summary for the Week of April 14, 2025*, https://www.cisa.gov/news-events/bulletins/sb25-111, (last accessed February 13, 2026).

[40] *Id.*

36. Despite TP-Link representing its networking devices protect consumers privacy and security, the experts have made the opposite clear. TP-Link's routers are rife with vulnerabilities which allow China access to consumers' homes and businesses, further heightening consumers' risk of a security breach. Though these issues have been reported on and warned of for years now, TP-Link's websites, blogs, and advertisements continue to falsely insist it "protects comprehensively."[42]

III. TP-Link's Mobile Applications Fail to Obtain Informed Consent

37. TP-Link's mobile applications collect consumers' personal data, claim to provide customization and control of their privacy and security settings. But TP-Link fails to disclose a critical fact: TP-Link's Chinese-affiliations require it to comply with PRC national intelligence laws mandating the disclosure of American consumer data.[43] 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.

[41] 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/, (last accessed February 13, 2026).

[42] TP-Link, Homeshield, https://www.tp-link.com/us/homeshield/, (last accessed on February 13, 2026).

[43] *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 accessed February 13, 2026).

38. 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, and grant consumers the ability to customize and control privacy and security settings. These apps are used in a wide-range of TP-Link networking and smart-home devices, such as cameras, fans, lights, and routers.

39. TP-Link's Kasa Smart app allows PRC to access consumers' personal information. TP-Link's Kasa app points to a "Kasa Privacy Policy(US)" that informs consumers of TP-Link's data collection and use practices.[44] Since at least January of 2024, this policy informs consumers of TP-Link's collection of data, including email, precise location, and mobile phone identifier. But, under its section titled "How we share personal data," TP-Link vaguely describes 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…"

40. China' 2017 National Intelligence law mandates all PRC companies and citizens support, assist, and cooperate with PRC intelligence efforts.[45] This law is applicable "domestically and abroad" according to the PRC.[46] The same law allows the PRC to "give commendations and awards" to individuals and organizations that do support PRC intelligence efforts.[47] TP-Link's

[44] App Store for iPhone, https://apps.apple.com/us/app/kasa-smart/id1034035493 (Kasa Smart application webpage) (last accessed February 16, 2026).
[45] *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 accessed February 13, 2026).
[46] *Id.*
[47] *Id.*

Chinese-ties in its supply-chain, and in its ownership structure through Jeffrey Chao, subject Texas consumers to a heightened data breach risk.

41. This required compliance is precisely what Rep. Moolenaar warned of in his letter to Sec. Raimondo discussing China's 2017 National Intelligence Law.[48]

42. Here, TP-Link obtains uninformed consent for its Kasa Smart application with its "Privacy Policy(US)" by knowingly omitting that TP-Link's Chinese-affiliations subject consumers' data to PRC access, because disclosure would deter consumers from downloading the application and submitting to its data collection practices. Without clear disclosure, consumers have not consented to TP-Link's deceptive data practices.

43. TP-Link employs this same deceptive omission across its entire suite of applications. Nearly each privacy policy is identical, allowing the collection of personal information such as email, precise location, and mobile phone identifier while allowing the share of information for "applicable law or legal process."[49], [50],[51] None of these policies discloses that TP-Links's Chinese affiliations subject American consumer data to potential access by PRC intelligence agencies. The vagueness is not crafty, it is deception.

VII. VIOLATIONS OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT

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

[49] TP-Link, Tether Privacy Policy (November 25, 2024), https://privacy.tp-link.com/app/Tether/privacy, (last accessed February 13, 2026).

[50] TP-Link, Deco Privacy Policy (January 5, 2026), https://privacy.tp-link.com/app/Deco/privacy, (last accessed February 13, 2026).

[51] TP-Link, Tapo Privacy Policy (October 18, 2024), https://privacy.tp-link.com/app/tapo/privacy, (last accessed February 13, 2026).

44. Texas incorporates the foregoing allegations as if set forth fully herein.

45. Texas Bus. & Com. Code § 17.47 authorizes the Consumer Protection Division to bring an action for temporary and permanent injunction whenever it has reason to believe that any person is engaged in, has engaged in, or is about to engage in any act or practice declared unlawful under Chapter 17 of the Business and Commerce Code.

Count I
Engaging in false, misleading, or deceptive acts or practices in the conduct of any trade or commerce.

46. Texas Bus. & Com. Code § 17.46(a) prohibits false, misleading, or deceptive acts or practices in the conduct of trade and commerce.

47. As alleged herein and detailed above, TP-Link has in the course and conduct of trade and commerce engaged in false, misleading, or deceptive acts or practices declared unlawful by and in violation of Section 17.46(a) and (b) of the DTPA.

Count II
False, Misleading, or Deceptive Acts Regarding TP-Link's Chinese-affiliations

48. Through false, misleading, or deceptive acts, either expressly or by implication, TP-Link misrepresents to Texas consumers that its software and devices are not affiliated with China, while knowing that its ownership and supply chain are Chinese; and while knowing that it receives benefits and awards from the Chinese government.

49. Through its false, misleading, or deceptive acts, TP-Link has violated the following DTPA Sections:

- 17.46(a) which prohibits "[f]alse, misleading, or deceptive acts or practices in the conduct of any trade or commerce;"

- 17.46(b)(5) which prohibits "representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not have;" and

- 17.46(b)(24) which prohibits "failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction which the consumer would not have entered had the information been disclosed".

Count III
False, Misleading, or Deceptive Acts Regarding TP-Link's Privacy and Security Representations

50. Through false, misleading, or deceptive acts, either expressly or by implication, TP-Link misrepresents to Texas consumers that its software and devices are secure, while knowing that its networking and smart home devices contain security vulnerabilities; and while knowing that Chinese data laws require TP-Link to allow the PRC access to Texas consumers' data.

51. Through its false, misleading, or deceptive acts, TP-Link has violated the following DTPA sections:

- 17.46(a) which prohibits "[f]alse, misleading, or deceptive acts or practices in the conduct of any trade or commerce;"

- 17.46(b)(5) which prohibits "representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not have;"

- 17.46(b)(7) which prohibits "representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another"; and

- 17.46(b)(12) which prohibits "representing that an agreement confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law."

- 17.46(b)(24) which prohibits "failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed".

Count IV
False, Misleading, or Deceptive Acts Regarding TP-Link's Country of Origin Labels

52. Through false, misleading, or deceptive acts, either expressly or by implication, TP-Link deceives Texas consumers as to the country of origin of TP-link's devices by including "Made in Vietnam" labels on devices that all or virtually all of the components are not from Vietnam; and by including "Made in Vietnam" labels on devices that all or virtually all of the components are imported from China.

53. Through its false, misleading, or deceptive acts, TP-Link has violated the following DTPA sections:

- 17.46(a) which prohibits "[f]alse, misleading, or deceptive acts or practices in the conduct of any trade or commerce;"

- 17.46(b)(4) which prohibits "using deceptive representations or designations of geographic origin in connection with goods or services."

- 17.46(b)(5) which prohibits "representing that goods or services have sponsorship, approval, characteristics, ingredients uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not;"

- 17.46(b)(24) which prohibits "failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information

was intended to induce the consumer into a transaction which the consumer would not have entered had the information been disclosed".

VIII. CIVIL PENALTIES

54. Texas incorporates the foregoing allegations as if set forth fully herein.

55. Texas is not required to allege injuries to bring claims seeking civil penalties under the DTPA. Tex. Bus. & Com. Code § 17.47(a) (creating a cause of action "[w]henever the consumer protection division has reason to believe that any person is engaging in, has engaged in, or is about to engage in any act or practice declared to be unlawful by [the DTPA] …"); *see e.g. Holzman v. State*, No. 13-11-00168-CV, 2013 WL 398935, at *3 (Tex. App.—Corpus Christi2013, pet. denied) ("Moreover, it is not necessary for the State to allege any injury to a [consumer] to recover the civil penalties it seeks in its live petition."); *see also Texas v. Colony Ridge, Inc.*, Civil Case No. CV-H-24-0941, 2024 WL 4553111, at *8 (S.D. Tex. 2024) (same).

56. Texas is entitled to recover up to $10,000 for each violation of the DTPA. See Tex. Bus. & Com. Code § 17.47(c)(1).

57. Texas Bus. & Com. Code § 17.47(g) (emphasis added) provides that "In determining the amount of penalty imposed … the trier of fact *shall consider*:

(1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of any prohibited act or practice;

(2) the history of previous violations;

(3) the amount necessary to deter future violations;

(4) the economic effect on the person against whom the penalty is to be assessed;

(5) knowledge of the illegality of the act or practice; and

(6) any other matter that justice may require.

VIII. TEMPORARY RESTRAINING ORDER AND TEMPORARY INJUNCTION

58. Texas incorporates the forgoing allegations as set forth fully herein.

59. Generally, an applicant for a temporary restraining order or temporary injunction must plead and prove (1) a cause of action against the defendant; (2) a probable right to the relief sought; and (3) a probable, imminent, and irreparable injury in the interim.[52]

60. However, the Texas Supreme Court has held that "when it is determined that [a] statute is being violated, it is within the province of the district court to restrain it" so "[t]he doctrine of balancing the equities has no application to this statutorily authorized injunctive relief."[53]

61. And "when an applicant relies upon a statutory source for injunctive relief . . . the statute's express language supersedes the common law injunctive relief elements such as imminent harm or irreparable injury and lack of an adequate remedy at law."[54]

62. Even so, the State's inability to enforce its "duly enacted [laws] clearly inflicts irreparable harm on the State."[55]

---

[52] *Butnaru v. Ford Motor Co.*, 84 S.W.3d 198, 204 (Tex. 2002); *Polston v. State*, No. 03-20-00130-CV, 2022 WL 91974, at *3 (Tex. App.—Austin Jan. 6, 2022, no pet.); *Trove v. Scott*, No. 03-99-00118-CV, 1999 WL 546997, at *1 (Tex. App.—Austin July 29, 1999, no pet.) (not designated for publication); Tex. R. Civ. P. 680.

[53] *State v. Texas Pet Foods, Inc.*, 591 S.W.2d 800, 805 (Tex. 1979).

[54] *West v. State*, 212 S.W.3d 513, 519 (Tex. App.—Austin 2006, no pet.); *see White Lion Holdings, L.L.C. v. State*, No. 01-14-00104-CV, 2015 WL 5626564, at *9 (Tex. App.—Houston [1st Dist.] Sept. 24, 2015, pet. denied) (mem. op.).

[55] *Texas Ass'n of Bus. v. City of Austin*, 565 S.W.3d 425, 441 (Tex. App.—Austin 2018, pet. denied) (quoting *Abbott v. Perez*, 585 U.S. 579, 602 (2018)); *see Washington v. Associated Builders*

63. This Court may issue a temporary restraining order with or without notice to the opposing party, while a temporary injunction requires notice.[56]

64. Whether to grant a temporary restraining order or temporary injunction rests with a trial court's sound discretion.[57]

65. The purpose of a TRO is to maintain the status quo pending a full hearing on the merits, not to order the complete relief sought.[58] The same is true of a temporary injunction.[59]

66. The Attorney General is charged with pursuing an action for a temporary restraining order, temporary injunction, or permanent injunction to prevent and restrain any violations of DTPA section 17.46(a)–(b).

67. Under the DTPA Texas needs only prove the following to obtain a temporary restraining order and temporary injunction against TP-Link: (1) that the Attorney General has reason to believe it is engaging in, has engaged in, or is about to engage in any act or practice declared to be unlawful by the DTPA, and (2) that proceedings would be in the public interest.[60]

& Contractors of S. Tex. Inc., 621 S.W.3d 305, 319 (Tex. App.—San Antonio 2021, no pet.) ("Like the trial court, our sister court, and the Supreme Court, we agree that the 'inability [of a state] to enforce its duly enacted [laws] clearly inflicts irreparable harm on the State.'" (quoting *Abbott*, 585 U.S. at 602 n.17, and *Texas Ass'n of Bus.*, 565 S.W.3d at 441)).

56 *See* Tex. R. Civ. P. 680–81.

57 *In re MetroPCS Communications, Inc.*, 391 S.W.3d 329, 336 (Tex. App.—Dallas 2013, no pet.); *Butnaru*, 84 S.W.3d at 204.

58 *In re Triantaphyllis*, 68 S.W.3d 861, 869 n.7 (Tex. App.—Houston [14th Dist.] 2002, no pet.) (citation omitted).

59 *Intercont'l Terminals Co., LLC v. Vopak N. Am., Inc.*, 354 S.W.3d 887, 891 (Tex. App.—Houston [1st Dist.] 2011, no pet.).

60 *West*, 212 S.W.3d at 518–19; *see also* Tex. Bus. & Com. Code § 17.47(a).

68. Deceptive acts in section 17.46(b) is non-exhaustive and a restraining order is appropriate if Defendants engaged in any "[f]alse, misleading, or deceptive act[] or practice[]."[61]

69. The fact that an entity has, or may, cease its unlawful conduct does not affect the State's entitlement to injunctive relief. [62]

70. The DTPA itself creates a conclusive presumption that potentially violative conduct coupled with a public need presents a sufficient risk of harm.

71. The Attorney General has reason to believe that TP-Link is engaging in, has engaged in, or is about to engage in any act or practice declared to be unlawful by the DTPA and that a temporary restraining order and a temporary injunction would be in the public interest. The severity and urgency of the public interest is demonstrated by Governor Abbott's designation of TP-Link as a prohibited technology to protect Texans from the threat posed by Chinese Communist Party. Consequently, this Court should immediately enter a temporary restraining order enjoining TP-Link and its officers, agents, servants, employees, and attorneys, and those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise, from collecting, selling, disclosing, using, or sharing Texas consumers' data it collects from TP-Link networking and smart home devices.

IX. RIGHT TO ISSUE WITHOUT BOND

72. State requests that the Clerk of the court issue such Writs of Injunction pursuant to any Injunction issued by this Court in conformity with the law, and that the same be issued and be

---

61 Tex. Bus. & Com. Code § 17.46(a).

62 *West*, 212 S.W.3d at 518–19.

effective without the execution and filing of a bond, as the State is exempt from such bonds under § 17.47(b) of the Texas Business and Commerce Code.

X. TRIAL BY JURY

73. Texas Demands a jury trial and tenders the appropriate fee with this petition.

XI. PRAYER FOR RELIEF

74. Texas respectfully requests that this Court enter judgment awarding the following for TP-Link's violations of the DTPA:

a. Finding that TP-Link has violated §§ 17.46(a) and (b) of the DTPA by engaging in the false, misleading, or deceptive acts or practices alleged above;

b. Requiring Defendants to pay civil penalties of up to $10,000 per violation of the DTPA as authorized by Tex. Bus. & Com. Code § 17.47(c)(1);

c. If the act or practice that is the subject of the proceeding was calculated to acquire or deprive money or other property from a consumer who was 65 years of age or older when the act or practice occurred, an additional amount not more than $250,000 as authorized by § 17.47(c)(2);

d. Temporarily and permanently enjoin TP-Link, its agents, employees, and all other persons acting on its behalf, directly or indirectly from engaging in false, misleading, or deceptive acts and practices, including but not limited to:

    1) Enjoin TP-Link from making false, misleading or deceptive representations that TP Link products are "Made in Vietnam";

2) Order TP-Link to represent to the public that TP-Link networking and smart home devices are "Made in China";

3) Order TP-Link to make clear and conspicuous representations to American consumers who use TP-Link networking and smart home devices' that they have ties to China;

4) Enjoin TP-Link directly or indirectly from representing to Texas consumers, in relation to the sale of TP-Link's networking and smart home devices, that TP-Link's products are secure; and

5) Enjoin TP-Link from collecting, sharing, selling, using, or disclosing consumers' data without providing customers with a clear and conspicuous notice of TP-Link's practices and obtaining customers' express, informed consent.

e. Requiring TP-Link to pay all attorneys' fees and costs for the prosecution and investigation of this action, as authorized by Tex. Gov't Code Ann. § 402.006(c); and

f. The State be awarded any further relief to which it demonstrates entitlement under the law.

Respectfully submitted,

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER

First Assistant Attorney General

RALPH MOLINA
Deputy First Assistant Attorney General

AUSTIN KINGHORN
Deputy Attorney General for Civil Litigation

JOHNATHAN STONE
Chief, Consumer Protection Division

/s/ Jerry Bergman
JERRY BERGMAN
Deputy Chief, Consumer Protection Division
Texas State Bar No. 24081694

OFFICE OF THE ATTORNEY GENERAL OF TEXAS
Consumer Protection Division
P.O. Box 12548
Austin, Texas 78711
Telephone: (512) 463-2185
Fax: (512) 473-8301
Johnathan.Stone@oag.texas.gov
Jerry.Bergman@oag.texas.gov

ATTORNEYS FOR THE STATE

VERIFICATION

Pursuant to Tex. Civ. Rem. & Prac. Code § 132.001(f), Jerry Bergman submits this unsworn declaration in lieu of a written sworn declaration, verification, certification, oath, or affidavit required by Texas Rule of Civil Procedure 682. I am an employee of the following governmental agency: Texas Office of the Attorney General. I am executing this declaration as part of my assigned duties and responsibilities.

I declare under penalty of perjury that the factual allegations in this motion are true and correct.

Executed in Travis County, State of Texas, on the 17th day of February 2026.

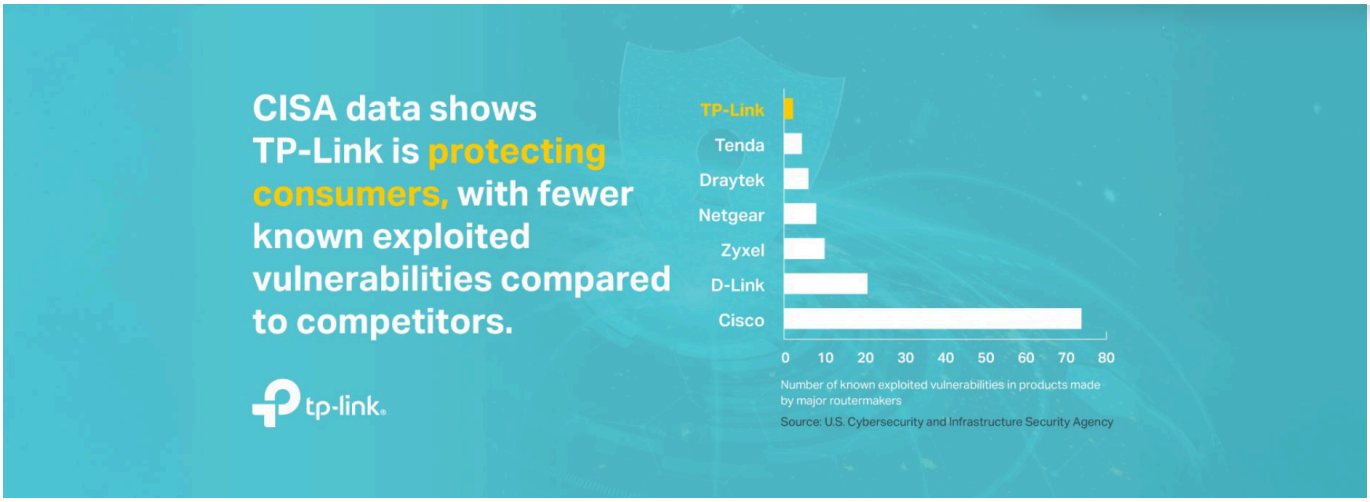
/s/ Jerry Bergman
Jerry Bergman

EXHIBITS

In support of the foregoing Plaintiff's Original Petition, attached are the following affidavits and exhibits, which are hereby incorporated by reference:

Exhibit A, TP-Link_CID_00056
Exhibit B, TP-LINK_CID_00074

EXHIBIT A



As a strong proponent of product security and user privacy protections, TP-Link has developed a comprehensive security framework designed to anticipate, identify, and address risks quickly and transparently.

To validate its security practices, TP-Link engaged Finite State, an independent U.S. cybersecurity firm, to conduct a thorough audit of its security investments in 2024. The audit found that TP-Link is on par with or ahead of other major industry players in terms of security outcomes. Public vulnerability data shows that TP-Link's rate of vulnerabilities per product is significantly lower than those of peer manufacturers, and its average CVSS score aligns with industry leaders.

"TP-Link Systems has demonstrated a strong commitment to security by investing in robust practices and embracing independent validation," said Matt Wyckhouse, Founder & CEO of Finite State. "Their proactive approach to identifying and addressing vulnerabilities sets a high standard for the industry, and their results speak for themselves."

Secure Manufacturing and Supply Chain

Since 2018, TP-Link has manufactured its U.S.-bound products in its own factory in Vietnam, ensuring greater control over its supply chain and adding an extra layer of security and governance.

"Manufacturing our products in our own facilities allows us to maintain the highest levels of quality and security," said Barney. "We are constantly assessing potential risks to our operations, customers, and supply chain to ensure we deliver safe and reliable products that our customers can trust."

Robertson to Lead Security Initiatives

Adam Robertson brings 17 years of cybersecurity experience to TP-Link, including eight years in senior leadership roles at companies like Reliance, Inc. and Incipio Group. Based at the company's global headquarters in Irvine, California, he will oversee security for TP-Link's consumer and enterprise networking and home automation products. His leadership will help further shape the company's security culture and accelerate innovation in cybersecurity.

"Adam's pragmatic approach to cybersecurity is exactly what TP-Link needs as we continue to innovate and expand our product offerings," said Barney. "His ability to balance technical depth with strategic vision will be invaluable as we work to elevate our security standards and set new benchmarks in the industry."

"I am excited to join TP-Link and contribute to its mission of making secure technology accessible to everyone," said Robertson. "I look forward to building on our world-class security team and ensuring that the TP-Link brand remains synonymous with trust and security in the technology industry."

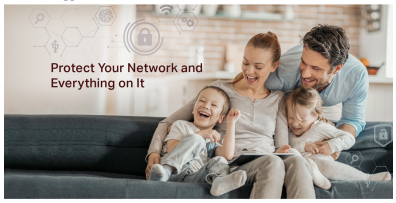
Cutting-Edge Network Security with TP-Link HomeShield

As part of TP-Link's ongoing commitment to product security, HomeShield provides an additional layer of prote

EXHIBIT B

HomeShield

overview support



HomeShield Let the Experts Secure Your Home

Customize your home network with enhanced security using a kit of features built in TP-Link HomeShield. Whether protecting your sensitive data or limiting the access of kids and guests, HomeShield provides you the tools you need to fully manage your network.

Real-Time IoT Protection | Network Protection | Robust Parental Controls | Comprehensive Reports

Care About All Your Concerns

Private Info Leakage | Cyber Virus Intrusion | Teenager Internet Addiction | IoT Devices Attacks

Real-Time IoT Protection

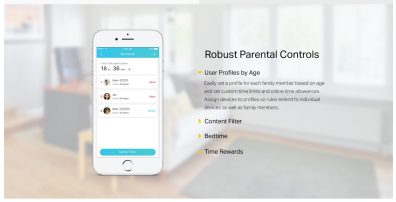
TP-Link HomeShield identifies IoT devices and immediately begins monitoring their security performance once they join the network. With a firewall, HomeShield blocks unauthorized access, encrypts your data, and protects against cyber threats and attacks.

- Identify IoT Devices
- Security Scanning for IoT

Network Protection, 100% Safeguard

- Malicious Site Blocker
- Intrusion Prevention System
- Home Network Scanner

Provides a real-time network scanner for your home WiFi to detect potential threats and warns security issues in the first place.



Robust Parental Controls

- User Profiles by Age

Easily add a profile for each family member based on age and set custom time limits and online time allowances. Assign devices to profiles so rules extend to individual devices as well as family members.

- Content Filter
- Bedtime
- Time Rewards

Comprehensive Reports

More detailed reports to help you get a complete understanding of your home WiFi and each connected device.

Internet Use Overview

Get a complete understanding of your home network security and your family's online behavior.

Customizable Quality of Service

With QoS, you can assign bandwidth to the devices you use most, keeping them running their best. Simple controls let you prioritize bandwidth for streaming, gaming, surfing or video chatting.

Device Priority

Choose which devices always have the fastest connections, or set a schedule to assign device priority for different times of the day.

Features		HomeShield	
		Basic FREE	Pro
IoT	IoT Device Identification	✓	✓
	IoT Device Security	-	✓
Network Protection	Network Security Scan	✓	✓
	Public WiFi Scan	✓	✓
	Malicious Content Filtering	-	✓
	ID-Theft Protection	-	✓
	Port Intrusion Prevention	-	✓
QoS	QoS Device Prioritization	✓	✓
Parental Controls	User Profiles	10 family members	10 family members
	Time Limits	-	✓
	Bedtime	Set one fixed time	Set different times for different days
	Offline	-	✓
	Time Rewards	-	✓
	Block Websites	✓	✓
	Professional Content Filter	✓	✓
	Traffic Statistics	-	✓
	Parent Permitted	✓	✓
Reports	New Wireless Devices Statistics	✓	✓
	Device Type Statistics	-	✓
	Safety Statistics	-	✓
	Online Time Analysis	-	✓
	Website URLs Analysis	-	✓
	Overview of Children's Information	-	✓
	Insight	1 days	30 days
Notice	Weekly/Monthly Reports	✓	✓
	URLs Interception	✓	✓
	Security Reminder and Scan	-	✓
	Subscription Expiration Notice	-	✓
	Security Events	-	✓

Supported Models

Tri-Band Mesh Wi-Fi 6 System
Deco X90

Tri-Band Mesh Wi-Fi 6 System
Deco X60

See More >

Deco | Router

HomeShield at Your Fingertips

Create personalized network settings for each member of your family with the Deco or Tether app.

TP-LINK_CID_00074