KRISTIN K. MAYES
ATTORNEY GENERAL
(Firm State Bar No. 14000)
Telephone: (602) 542-3725
Facsimile: (602) 542-4377
Email: consumer@azag.gov
Plaintiff State of Arizona

Additional counsel for Plaintiff on signature page

SUPERIOR COURT OF ARIZONA
IN MARICOPA COUNTY

STATE OF ARIZONA, *ex rel.* KRISTIN K. MAYES, Attorney General, Plaintiff, v. PDD HOLDINGS, INC., F/K/A PINDUODUO INC.; and WHALECO, INC., D/B/A TEMU, Defendants.	Case No. **COMPLAINT** (Jury Trial Demanded)

Plaintiff, the State of Arizona *ex rel.* Kristin K. Mayes, the Attorney General ("Arizona" or "the State"), brings this action against Defendants PDD Holdings Inc. f/k/a Pinduoduo Inc. and Whaleco Inc. d/b/a Temu ("Temu") (collectively, "Defendants"), for violations of the Arizona Consumer Fraud Act, Arizona Revised Statutes ("A.R.S.") §§ 44-1521 to 44-1534 ("ACFA"). In support of its claims, the State alleges the following for its Civil Complaint (the "Complaint"):

I. INTRODUCTION

1. This is a consumer protection action brought to redress and restrain violations of the ACFA, pursuant to which the State seeks an order enjoining Defendants' conduct challenged herein, imposing civil penalties, requiring restitution, and providing all other equitable relief to which the State is entitled.

2. The harms committed against Arizona by Defendants are multifold. This Complaint challenges two separate types of conduct, which in turn yield two separate types of harms. Accordingly, there are two, distinct parts of the Complaint, each of which addresses these respective harms.

3. The first harm, discussed in Sections IV.A through .I of this Complaint (¶¶ 47–200) involves threats to Arizonans' privacy and security due to code-level behaviors in the Temu app which the State's investigation has uncovered. These behaviors collect users' sensitive personally-identifiable information ("PII") without their knowledge or consent. These privacy and security harms are compounded both because the Temu app is purposely designed to evade detection—even going so far as being able to reconfigure itself and its properties on an individual's phone without anyone's knowledge (other than Defendants'), and because Defendants—by their own acknowledgement—have a portion of their operations located on mainland China, where cybersecurity laws allow the government unfettered access to data owned by Chinese businesses whenever it wishes. While the surreptitious collection of data—and nothing else—is a violation of the ACFA, this additional geopolitical component amplifies the consequences of that existing violation.

4. The second harm, discussed in Section IV.J of the Complaint (¶¶ 201–254), involves more traditional consumer deception. Temu sells products to Arizonans in ways that are plainly violative of the ACFA, injuring those citizens, accordingly.

5. In 2022, Defendants launched Temu, an online shopping platform in the United States. The Temu mobile application and website (the "Temu platform" or "Temu app"), allows users to purchase low-cost goods manufactured in China.

///

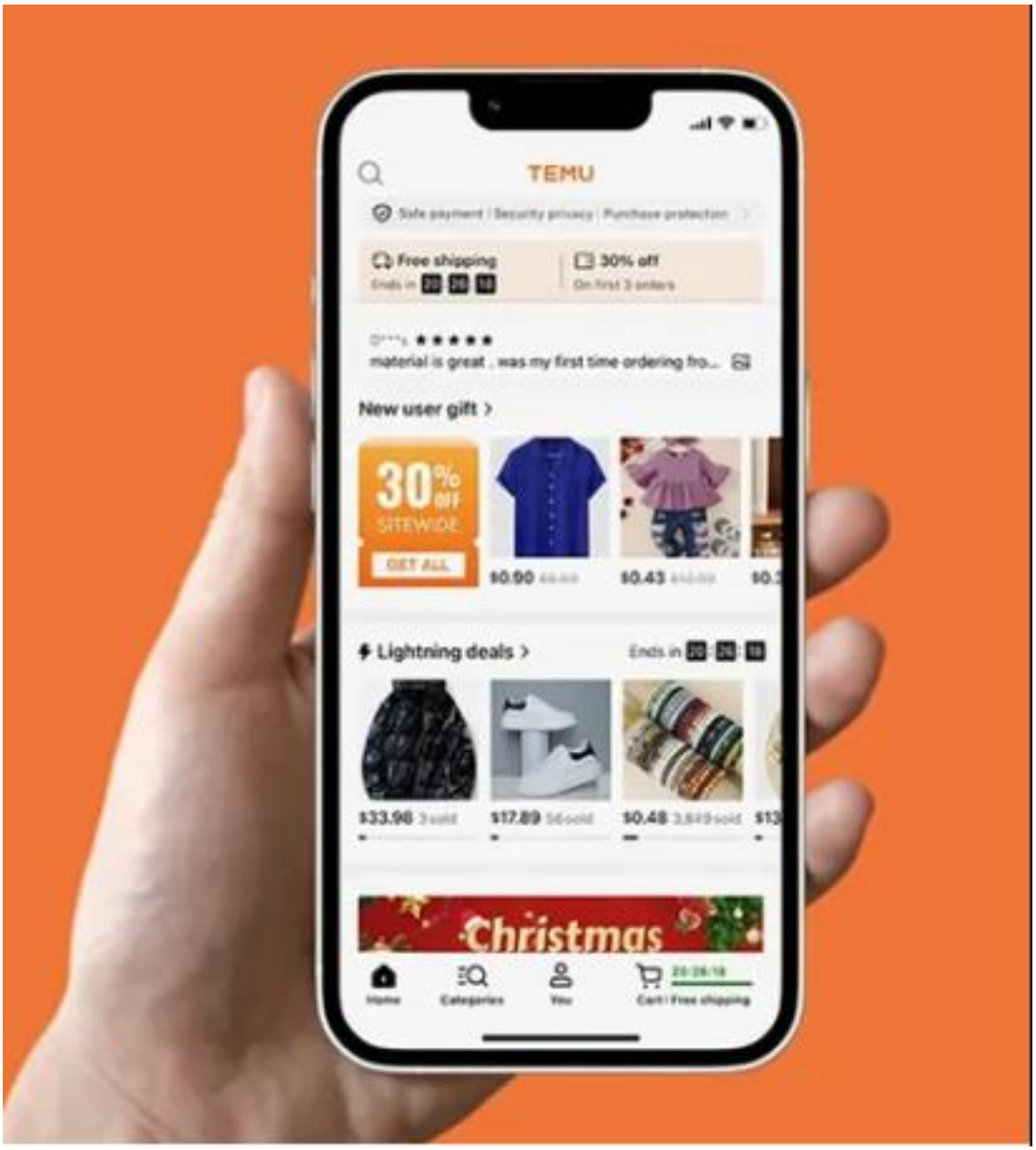

Figure 1: Representation of the Temu mobile application.

6. Temu is ultimately owned by the Nasdaq-listed Chinese company PDD Holdings Inc., which runs the Chinese e-commerce giant Pinduoduo, an online shopping platform that was the precursor for the Temu platform (the "Pinduoduo platform" or "Pinduoduo app").

///

///

Figure 2: Representation of the Pinduoduo mobile application.

7. The Temu app is wildly popular throughout the United States, including in the State of Arizona, with usage driven both via word of mouth and by an aggressive, multibillion-dollar marketing campaign. This campaign recently made headlines for three separate advertisements that Temu aired during the 2024 Super Bowl, as well as two additional advertisements aired immediately following the game.[1] The advertisements "featured animated characters using the app to transform their lives to the tune of a catchy jingle. The marketing campaign urged viewers…to 'shop like a billionaire' as the ad's avatars filled their homes with $10 toasters and $6 skateboards."[2]

8. In 2023, Temu was the most downloaded app in the U.S.,[3] with users spending almost twice the amount of time on the platform than on rival Amazon.[4]

9. But Temu is more than an e-commerce juggernaut. Within the last year, a host of security and privacy concerns have been raised about both the Temu app and the Pinduoduo app.

10. In March 2023, Google suspended the Pinduoduo app (the forerunner of Temu and the app of its parent company) from its Google Play Store after it was found to contain malware.[5] Similarly, in mid-2023, Apple suspended the Temu app from the Apple App Store for

---

[1] Erin Snodgrass, *Temu dropped tens of millions of dollars on its flurry of Super Bowl ads — and its big spending may pay off*, Business Insider (Feb. 12, 2024, 11:43 PM), https://www.businessinsider.com/temu-spends-millions-super-bowl-ads-effort-win-us-users-2024-2.

[2] *Id*.

[3] Sarah Perez, *Temu was the most-downloaded iPhone app in the US in 2023*, TechCrunch (Dec. 12, 2023, 8:47 AM), https://techcrunch.com/2023/12/12/temu-was-the-most-downloaded-iphone-app-in-the-u-s-in-2023/.

[4] Jinshan Hong, *Shoppers Spend Almost Twice as Long on Temu App Than Key Rivals*, Bloomberg (Dec. 12, 2023, 2:43 AM), https://www.bloomberg.com/news/articles/2023-12-12/shoppers-spend-almost-twice-as-long-on-temu-app-than-rivals-like-amazon?sref=gni836kR.

[5] Helen Davidson, *Addictive, absurdly cheap and controversial: the rise of China's Temu app*, The Guardian (Oct. 5, 2023, 10:26 PM), https://www.theguardian.com/world/2023/oct/06/addictive-absurdly-cheap-and-controversial-the-rise-of-chinas-temu-app.

misrepresentations Temu had made about the types of data the app can access or collect from users, how it does so, and for what purposes it uses that data.[6]

11. Consequently, news outlets and technologists engaged in their own investigations of the Temu app. These investigations—involving review of the Temu app source code, documentation, network traffic and/or other dynamic or static analyses, along with interviews of company insiders—revealed that the Temu app has multiple hallmarks of spyware and malware, and engages in practices that are neither necessary nor appropriate for an e-commerce app.

12. The State has conducted its own independent forensic investigation of the Temu app. This investigation examined the code of both the Temu app and its predecessor, the Pinduoduo app, and focused on the ways in which each app has code and functionality overlap.

13. Independent of any code overlay between Temu and Pinduoduo, the State separately and extensively conducted both static and dynamic analysis of the Temu app over time. This means that the State forensically reviewed both what the Temu app is designed to do and how it operates when used by account holders.

14. Except where specifically noted, all factual allegations in this Complaint about the technical design, functionality, and features of the Temu app are based on the State's own independent forensic investigation and do not rely or depend on any outside forensic analysis.

15. In all instances, the State's investigation revealed that the Temu app is designed to collect sensitive user data without the user's knowledge or consent and is purposely designed to evade detection of this type of data collection by third-party security researchers.

16. For example, Temu collects an alarming amount of sensitive user data and personally-identifiable information ("PII") that is well beyond what would be necessary in the ordinary course of business for an online shopping app. Examples include a user's granular geolocation ("GPS"), lists of all other installed apps and associated accounts on consumer's

[6] Clothilde Goujard, *Booming Chinese shopping app faces Western scrutiny over data security*, Politico (Jul. 24, 2023, 12:00 PM), https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/.

phones, and the cellular data and WiFi networks the user's phone is connected to as well as all WiFi networks that are detected by the user's mobile device.

17. This exfiltration of data happens without a consumer's knowledge or consent. Beyond merely failing to disclose the depth and breadth of its data collection practices to consumers, Temu actively seeks to prevent its conduct from being discoverable.

18. In fact, a review of the Temu app's code shows that it is purposely designed to evade front-end security review. The app applies multiple layers of encryption to its various processes, in an effort to shield itself from forensic review. It also uses code to "sniff out" potential forensic tools or settings in order to determine whether it is being examined by a third-party reviewer. The app is even able to go so far as to edit its own code once it has been downloaded to a consumer's phone, potentially allowing it to exploit user's PII and other data, or to otherwise control the consumer's device, in unknown and unknowable ways.

19. These privacy and security risks are compounded by the fact that Temu is owned by a Chinese company (PDD Holdings, Inc.), which itself is subject to Chinese law, including laws that mandate secret cooperation with China's intelligence apparatus, to the exclusion of any data protection guarantees existing in the United States.

20. The sensitive PII that Temu collects from Arizona citizens is accessible by individuals and entities subject to Chinese law and beholden to China's regime, including but not limited to laws requiring cooperation with China's national intelligence institutions and cybersecurity regulators. Chinese government officials have interpreted Chinese law as applying to any data in which China has a national intelligence or security interest, no matter where the data is located. In other words, it can reasonably be assumed that the data Temu is illicitly collecting from Arizona users is being sent to and used by the Chinese government.

21. Such concerns regarding data security and privacy endemic to Temu and other Chinese-owned apps have led government entities to ban or restrict their use. For example, the State of Montana recently banned the Temu app—along with other popular apps that are "tied to foreign adversaries" such as TikTok, WeChat, and Telegram—from government devices due

///

to the significant threats posed to users' security and privacy.[7] Likewise, Defendants are currently the subject of a congressional investigation based on "concerns about Temu and the amount of data collected."[8]

22. Defendants have sought to maximize their access to and collection of users' PII—both for profit and potentially for more nefarious geopolitical objectives—by employing unfair and deceptive trade practices. The app is designed, essentially, to hack consumers' mobile devices the moment it is downloaded, acquiring access to troves of sensitive information for which it has no need, in ways that are uniformly and indisputably associated with pernicious spyware and malware.

23. In addition to Defendants' unsafe and illicit data collection, the Temu app is awash in products that baldly infringe upon, or simply copy outright, intellectual property owned by U.S.-based businesses large and small.[9] As of the date of this filing, Temu features dozens of what appear to be unlicensed products claiming to be from Arizona brands like the Arizona Cardinals, Fender Guitars, Ping Golf, the University of Arizona, and Arizona State University.

24. Accordingly, the State brings this action pursuant to the ACFA and seeks a permanent injunction preventing Defendants from acquiring, maintaining, and otherwise utilizing the PII of Arizona citizens, preventing Defendants from allowing widespread intellectual property infringement to the detriment and confusion of Arizona consumers, and further seeks civil penalties in light of Defendants' conduct, as well as all other available relief allowed by law.

---

[7] Marvie Basilan, *After TikTok, Montana Bans WeChat, Temu And Telegram From Government Devices*, International Business Times (May 18, 2023, 4:32 AM), https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government-devices-3694060.

[8] Letter from Cathy McMorris Rodgers & Gus M. Bilirakis, United States Congress Committee on Energy and Commerce, to Mr. Qin Sun, President of Whaleco, Inc. d/b/a Temu and Pinduoduo (Dec. 20, 2023) (available at https://d1dth6e84htgma.cloudfront.net/CCP_Marketplace_Letter_to_Whaleco_Inc_Temu_7f921e1a67.pdf).

[9] Andrew R. Chow, *Designers are Accusing Temu of Selling Copies of Their Work*, TIME (Jan. 16, 2024, 8:43 AM), https://time.com/6342387/temu-copy-work/.

II. JURISDICTION AND VENUE

25. The State brings this action pursuant to the ACFA to obtain injunctive relief to permanently enjoin and prevent the unlawful acts and practices alleged in this Complaint, and to obtain other relief, including restitution, disgorgement of profits, gains, gross receipts, or other benefits, civil penalties, and costs and attorneys' fees.

26. This Court has personal jurisdiction over the Defendants, as they conduct business in Arizona and have purposefully availed themselves of this forum by conducting business in the State and by causing harm as a direct and proximate result of their actions. The Defendants regularly transacted and/or solicited business in the State and/or derived substantial revenue from goods used or consumed or services rendered in the State and/or contracted to supply goods or services in the State and/or caused injury by an act or omission in the State and/or caused injury in the State by an act or omission outside the State. At all times relevant to this Complaint, Defendants were, and still are, in trade and commerce affecting Arizona consumers insofar as they operate the Temu app which has been intentionally directed towards, marketed to, and downloaded by citizens of the State. Defendants have engaged in myriad commercial transactions with Arizona consumers, taking payment from consumers in Arizona-based commercial transactions and sending various products to Arizona consumers. Defendants were—and remain—in possession of and/or have or have had control over sensitive PII of Arizona citizens. Defendants have the requisite minimum contacts with Arizona necessary to permit this Court to exercise jurisdiction.

27. This Court has subject matter jurisdiction over this matter, including under Article VI, Section 14, of the Arizona Constitution.

28. This Court may issue appropriate orders both prior to and following a determination of liability pursuant to A.R.S. § 44-1528.

29. Arizona does not plead any cause of action or request any remedy arising under or founded in federal law. The instant Complaint does not confer diversity jurisdiction upon the federal courts pursuant to 28 U.S.C. § 1332. The State is not a citizen of any state.

///

30. Likewise, federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331 is not invoked by the Complaint, as it sets forth herein exclusively viable state law claims against Defendants. Nowhere herein does the State plead, expressly or implicitly, any cause of action or request any remedy that arises under federal law. The issues presented in the allegations of this Complaint do not implicate any substantial federal issues and do not turn on the necessary interpretation of federal law. No federal issue is important to the federal system as a whole under the criteria set by the Supreme Court in *Gunn v. Minton*, 568 U.S. 251 (2013).

31. Specifically, the causes of action asserted, and the remedies sought herein, are founded upon the positive statutory, common, and decisional laws of Arizona. Further, the assertion of federal jurisdiction over the claims made herein would improperly disturb the congressionally approved balance of federal and state responsibilities. Accordingly, any exercise of federal question jurisdiction is without basis in law or fact.

32. In this Complaint, to the extent Arizona cites or alludes to federal statutes, regulations, or agency memoranda, it does so only to establish Defendants' knowledge, to state the duties owed under Arizona law, or to explain the hybrid nature of industry oversight, not to allege an independent federal cause of action and not to allege any substantial federal question under *Gunn v. Minton*.

33. Venue is appropriate in Maricopa County pursuant to A.R.S. § 12-401(17).

III. PARTIES

A. The State of Arizona

34. Plaintiff is the State of Arizona *ex rel.* Kristin K. Mayes, the Attorney General of Arizona, who is authorized to bring this action under the ACFA.

B. PDD Holdings Inc., f/k/a Pinduoduo Inc.

35. Defendant PDD Holdings Inc. ("PDD Holdings") was founded in China in 2015 under the name Pinduoduo, and is registered in the Cayman Islands. It owns and operates a portfolio of businesses both in China and the United States. Among other things, PDD Holdings owns and operates the Pinduoduo e-commerce platform that offers various consumer products. PDD Holdings also owns the company that operates the Temu online marketplace (Co-

Defendant Whaleco, Inc., discussed *infra*). PDD Holdings was formerly known as Pinduoduo Inc., with headquarters in Shanghai, China. In February 2023, PDD Holdings moved its "principal executive offices" from Shanghai, China to Dublin, Ireland.[10] However, it continues to have significant operations in China, with multiple subsidiaries located within that country.

36. PDD Holdings is publicly traded on the NASDAQ stock exchange with the ticker name PDD, and files annual reports with the U.S. Securities and Exchange Commission ("SEC").

C. Whaleco Inc., d/b/a Temu

37. Defendant Whaleco Inc. ("Temu") is, and at all relevant times was, a corporation incorporated in Delaware and headquartered in Boston, Massachusetts. Temu is an online marketplace operated by Defendant PDD Holdings.

D. Alter Ego and Single Enterprise Allegations

38. Defendants do not function as separate and independent corporate entities. Defendant Temu is directly controlled by Defendant PDD Holdings.

39. At all relevant times, Defendant PDD Holdings has directed the operations of Defendant Temu with respect to the Temu app, and Defendant Temu has reported to Defendant PDD Holdings. Defendant PDD Holdings has made, and continues to make, key strategy decisions for Defendant Temu.

40. Defendant Temu and Defendant PDD Holdings have significant overlap of executive officers of each corporation.

41. Defendant PDD Holdings' most recent Form 20-F filing with the SEC states that the purpose of the Temu platform is to "primarily serve merchants in China, assisting them in reaching customers and growing sales."[11]

---

[10] Arjun Kharpal, *Tech giant PDD Holdings, parent of Pinduoduo and Temu, moves headquarters from China to Ireland*, CNBC (May 5, 2023, 1:42 AM), https://www.cnbc.com/2023/05/04/chinas-pdd-holdings-parent-of-temu-moves-headquarters-to-ireland.html.

[11] PDD Holdings, Form 20-F Annual Report (2024).

42. This "primary" purpose of the Temu platform is accomplished by Defendant PDD Holdings directing the operations of Defendant Temu in the United States, and the State of Arizona, to facilitate transactions between Arizona consumers and Chinese merchants in part using data and information gathered about Arizona consumers unlawfully, as described below.

43. Moreover, employees from PDD Holdings have performed work on the Temu app, including software engineers who previously developed the Pinduoduo app for PDD Holdings.

44. Defendants' Temu app contains significant code overlap with Defendants' Pinduoduo app, including proprietary code and app programming components copied directly from the Pinduoduo app into the Temu app that are central to Defendants' violation of the ACFA, discussed *infra* at ¶¶ 110–114.

45. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer, and/or alter ego of the other Defendant, and acted in the course and proper scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the acts or transactions of the other Defendant.

46. At all relevant times, and in connection with the matters alleged herein, Defendants constituted a single enterprise with a unity of interest. Notwithstanding this fact, as detailed further below, each Defendant is also directly liable based on its own actions independent of any alter ego or single enterprise theory of liability.

IV. FACTUAL BACKGROUND

A. Defendant PDD Holdings is a Chinese Online Retailer That, Through Its Pinduoduo and Temu Apps, Has Become One of the Largest E-Commerce Entities in the World.

47. Founded in 2015 by Chinese businessman, software engineer, and former Google employee Colin Huang, PDD Holdings is one of China's largest companies, generating an

///

///

estimated $383 billion in gross merchandise value (GMV) in 2021 alone.[12]

48. Among other business activities, PDD Holdings operates Pinduoduo, an e-commerce app created in China that offers consumer products across a spectrum of categories.

49. Pinduoduo was developed to compete with Chinese online retailers Alibaba and JD.com by selling low-priced goods. The Pinduoduo app serves as a marketplace that recruits China-based suppliers to offer products and provides a range of low-cost products to consumers who visit its site. As described in Pinduoduo's SEC filings, "[t]he platform pioneered an innovative 'team purchase' model. Buyers are encouraged to share product information on social networks, and invite their friends, family and social contacts to form shopping teams to enjoy the more attractive prices available under the 'team purchase' option. Pinduoduo's buyer base helps attract merchants to the platform, while the scale of the platform's sales volume encourages merchants to offer more competitive prices and customized products and services to buyers, thus forming a virtuous cycle."[13]

50. While the Temu app has not yet introduced the "team purchase" feature in the United States, Temu does offer significant discounts to users who invite their friends to download the app,[14] thus incentivizing the proliferation of the app on social media platforms.

51. PDD Holdings operates a series of subsidiaries in China and has long maintained its corporate headquarters in Shanghai, China. However, following a growing chorus of geopolitical security and privacy concerns, and to obscure its connections to China, PDD Holdings recently disclosed that it was moving its "principal executive offices" to Dublin, Ireland. Nonetheless, the vast majority of PDD Holdings' business operations, including several subsidiaries, continue to be located in China.

---

[12] Pinduoduo Inc., *Pinduoduo Announces Fourth Quarter 2021 and Fiscal Year 2021 Unaudited Financial Results* (Mar. 21, 2022), https://investor.pddholdings.com/news-releases/news-release-details/pinduoduo-announces-fourth-quarter-2021-and-fiscal-year-2021.

[13] PDD Holdings, Form 20-F Annual Report (2022).

[14] Planet Money, *What is Temu*, NPR (Mar. 22, 2024, 6:08 PM), https://www.npr.org/transcripts/1197958526?ft=nprml&f=1197958526.

B. The Pinduoduo App Has Been Deemed to Be Malware by Security Experts and Was Banned from Google's App Marketplace.

52. On March 21, 2023, Google suspended the Pinduoduo app from the Google Play Store after malware issues were found on the app.[15] Subsequently, independent security researchers were alarmed at what they uncovered when they examined the app's source code and its behavior once installed on mobile devices. For example, CNN conducted a detailed investigation in which it spoke to half a dozen cybersecurity teams from Asia, Europe and the United States, as well as multiple former and current Pinduoduo employees. According to those sources, "while many apps collect vast troves of user data, sometimes without explicit consent," Pinduoduo took "violations of privacy and data security to the next level."[16]

53. Among other things, the expert sources found that the app was programmed to bypass users' cell phone security in order to monitor and record a user's activities across their phone—and not just those activities that related to the app itself.[17]

54. For example, "the researchers found code designed to achieve 'privilege escalation': a type of cyberattack that exploits a vulnerable operating system to gain a higher level of access to data than it is supposed to have."[18]

55. According to one report by an IT security firm, "Pinduoduo requested as many as 83 permissions, including access to biometrics, Bluetooth, and Wi-Fi network information."[19]

---

[15] Baranjot Kaur & Abinaya Vijayaraghavan, *Google suspends China's Pinduoduo app on security concerns*, Inside Retail (Mar. 24, 2023), https://insideretail.asia/2023/03/24/google-suspends-chinas-pinduoduo-app-on-security-concerns/.

[16] Nectar Gan, Yong Xiong & Juliana Liu, *'I've never seen anything like this:' One of China's most popular apps has the ability to spy on its users, say experts*, CNN (Apr. 3, 2023, 5:16 AM), https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html.

[17] *Id.*

[18] *Id.*

[19] Nicholas Foisy, *Temu App Poses Potential Data Risk for Consumers*, Compass IT Compliance (June 30, 2023, 11:00 AM), https://www.compassitc.com/blog/temu-app-poses-potential-data-risk-for-consumers.

The purpose of this was, "to spy on users and competitors, allegedly to boost sales,"[20] according to a company insider.

56. The Pinduoduo app "also had the ability to spy on competitors by tracking activity on other apps [on the user's phone] and getting information from them," which is contrary to Apple's and Google's app store policies.[21]

57. In point of fact—according to a current Pinduoduo employee—"the company established a team of 100 engineers and product managers to dig for vulnerabilities in Android phones, develop ways to exploit them – and turn that into profit."[22]

58. This bears repeating: Pinduoduo hired a small army to figure out vulnerabilities in the Android operating system and then use those discovered vulnerabilities to secretly acquire users' PII in contravention of safeguards that Android had established. As discussed in paragraphs 108 through 112, *infra*, the work of this group continues to manifest itself in Temu, as well.

59. According to a company insider source, who requested anonymity for fear of reprisals, "[t]he goal was to reduce the risk of being exposed."[23]

60. Moreover, once the app was installed, the app was able to continue running in the background and prevent itself from being uninstalled.[24]

61. One security researcher interviewed by CNN described Pinduoduo as "the most dangerous malware ever found among mainstream apps."[25]

62. Analysts, including experts at Google, concluded that the Pinduoduo app was covertly collecting private and personal data from users without their knowledge and consent, including highly sensitive biometric data contained on users' devices. As discussed above, these functions were not accidental—they were intentionally built into the app.

---

[20] *Id.*
[21] Gan, Xiong & Liu, *supra* note 16.
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

63. Moreover, even after Defendants made changes to the Pinduoduo app in response to the suspension, they continued to violate users' privacy rights. For example, multiple security vendors continue to rate Pinduoduo as "malicious," as reported by the malware statistics service VirusTotal.com.

64. On March 5, 2023, Pinduoduo issued a new update of its app, version 6.50.0, which removed the exploits. Researchers who investigated the update said "although the exploits were removed, the underlying code was still there and could be reactivated to carry out attacks."[26]

65. Two days after the update, Pinduoduo disbanded the team of 100 engineers and product managers who had developed the exploits, according to a Pinduoduo source.[27]

66. Thereafter, most of the members on this team were transferred to work at Temu.[28]

C. In 2022, PDD Holdings Developed the Temu App, Which is Modeled on Pinduoduo—Including Through Its Design and Code—and Which Defendants Aggressively Marketed in the United States and Arizona.

67. In 2022, Defendants developed the Temu app, meant to be a global version of the Pinduoduo platform, with the United States as its principal market.[29]

68. Since that time, Defendants have heavily promoted the Temu app, including through television advertisements, large online ad campaigns, and sponsorships.

69. As described, *supra*, the same 100-member team of software engineers and product managers from Pinduoduo—whose principal mission was to identify exploitations in the Android operating system and incorporate them into the app—were transitioned to working on the Temu app within a year of Temu's introduction into the marketplace.[30]

---

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Goujard, *supra* note 5.
[30] Gan, Xiong & Liu, *supra* note 16.

70. Like the Pinduoduo app, the Temu app provides a marketplace for Chinese suppliers to offer their products. However, the Temu app also handles delivery, promotion, payment processing, and after-sales services for merchants on its platform. "Temu's network now includes more than 80,000 suppliers."[31]

71. As a result of Defendants' heavy promotion of the Temu app, it has experienced exponential growth. In 2023, Temu was the most downloaded app in the United States.[32] As a result, the market capitalization of Defendant PDD Holdings has swelled to nearly $185 billion as of September 23, 2025.[33]

72. Temu is responsible for tens of millions of shipments that are sent to the United States each year—including via purchases made, finalized, and received in Arizona—through Temu's network of more than 80,000 China-based sellers participating in its online marketplace.[34]

D. Precisely Like the Pinduoduo App, Defendants' Temu App Presents a Host of Undisclosed Privacy and Security Risks.

73. Just like the Pinduoduo app, Temu uses the inducement of low-cost goods to lure users into unknowingly providing near-limitless access to their PII. Such acts are deceptive and unfair practices under Arizona law.

74. This conduct came to light following the removal of the Pinduoduo app from Google's Play Store due to the presence of malware that exploited vulnerabilities in users' phone operating systems and allowed the app to not only gain access (undetected) to virtually all data stored on the phones, but also to recompile itself and potentially change its properties *once installed*, in a manner designed to avoid detection. *See, supra*.

75. Indeed, in or about that same time period, Apple expressed similar concerns about the Temu app, concluding that the app did not comply with Apple's data privacy standards and

---

[31] Staff of H.R. Select Comm. on the CCP, 118th Cong., Rep. on Fast Fashion and the Uyghur Genocide: Interim Findings, at 4 (2023).
[32] Perez, *supra* note 3.
[33] Yahoo!Finance, https://finance.yahoo.com/quote/PDD/ (last visited September 23, 2025).
[34] Staff of H.R. Select Comm. on the CCP, *supra* note 31, at 8.

that Temu was misleading users regarding how their data was being used: "[Apple] said it had found that Temu misled people about how it uses their data. Temu's so-called privacy nutrition labels—descriptions about the types of data an app can access, how it does so and what it uses them for—did not accurately reflect its privacy policy, said Apple. Temu also isn't letting users choose not to be tracked on the internet [which is an option that all apps in Apple's online marketplace are required to provide to users]."[35]

76. As one commentator observed following the State of Montana's decision to ban the Temu app, the app is "dangerous," due to the fact that it "bypasses phone security systems to read a user's private messages, make changes to the phone's settings, and track notifications."[36]

77. The State's own forensic investigation of the Temu app reveals a host of troubling conduct, including but not limited to the following:

a. The app is designed to allow for extensive data exfiltration from all corners of a user's mobile device.

b. The app is designed to hide its exfiltration of PII, both from users and even from any researcher who might be investigating the app's functionality.

c. The app contains multiple portions of code that are recognized by cybersecurity professionals as hallmarks of spyware and malware.

d. The app contains code that allows it to reconfigure itself even after having been downloaded to a user's phone, without the user's knowledge or consent.

e. The app incorporates large swaths of Pinduoduo's previously banned code, wholesale.

78. These concerns are addressed more fully as follows:

i. Design and Programming That Intentionally Evades Scrutiny

1. Dynamic recompilation using the "Manwe" tool

[35] Goujard, *supra* note 5.
[36] Basilan, *supra* note 7.

79. Multiple versions of the Temu app have a patching capability through a home-built framework known as "Manwe," which is an unpacking and patching tool (also called a software development kit or "SDK") also found in the malicious versions of Pinduoduo.

80. Manwe enables Temu to patch the app on the device, rather than through releasing updates via the Apple App Store or Google Play Store.

81. Instead of releasing updates only via the Apple App Store or Google Play Store, this code enables the app to change its behavior—including its functionality—*on the user's phone*, without the user being able to know, much less prevent, such a change.

82. This allows the Temu app to pass all required tests for approval into the Google Play Store or Apple App Store, while retaining the ability to reconfigure itself once it has been downloaded onto a user's device.

83. It thus becomes pointless for Google or Apple to vet Temu for security and privacy risks, because the app is capable of changing itself *after* going through those tests.

84. This is against app store policies, as it enables Temu to push unauthorized code via updates to user devices without Google's or Apple's knowledge—and of course, without the user's knowledge, either.

85. And, as noted below, Temu also borrowed code from Pinduoduo in the form of the ZipPatch library (*see* ¶ 113, *infra*), which also allows the app to update its code without pushing the update through Google or Apple.

2. Omission of data collection practices from the Temu app manifest file

86. Temu also has hidden its conduct by omitting requested permissions from the "manifest file" of the app.

87. A manifest file is required for every app,[37] and *must* contain certain information, including the "permissions that the app needs in order to access protected parts of the system or

[37] Android, *App manifest overview*, Developers – Guides, https://developer.android.com/guide/topics/manifest/manifest-intro (May 20, 2025).

other apps."[38] As Google explains on its webpage for Android developers, "Android apps must request permission to access sensitive user data, such as contacts and [text messages], or certain system features, such as the camera and internet access. Each permission is identified by a unique label."[39]

88. When a permission is omitted from the manifest file, the conclusion to be drawn is that the app is not interested in the functionality associated with that permission. However, in certain instances, Temu would either omit or remove the requested permission from the manifest, while still acquiring data that would be the purview of that permission.

89. The most glaring example involves location data. Starting no later than April 2023, Temu removed the permissions ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION from its manifest. The conclusion one draws from this is that Temu was *not* collecting location data from its users.

90. However, during this time, Temu still was actively collecting user location, including by acquiring data that can be used to infer both approximate and precise location. *See* ¶¶ 116–121, *infra*.

91. In other words, Temu was creating the impression that it did not want, collect, or use its customers' location data, but in reality, was getting the information from sources that it could avoid disclosing in the permission manifest.

92. It was not until version 2.4.1 of the app, released on or about September 8, 2023, that Temu reinserted these permissions into the app manifest. Tellingly, this change occurred *two days* after a report was published by a short-seller accusing Temu of a host of privacy-invasive conduct, including Temu's removal of ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION from the manifest.

3. Hiding previous versions of the Temu app and its files

93. In addition, Defendants have sought to cover their tracks by removing prior versions of files associated with the Temu app from the public domain. Many websites archive

[38] *Id.*
[39] *Id.*

Android Package Kits (APKs; the file format used to distribute and install mobile applications on Android devices) published in the Google Play Store, and it is common practice in the industry for developers to have prior APKs of their app exist on these sites. But Temu's app is typically absent from APK archives. Indeed, the historical Temu APKs have been removed from all websites within the jurisdiction of the U.S., suggesting that Temu may be resorting to illegal measures to keep its historical APKs out of these archives. Inaccessibility of the APK files makes investigative research more cumbersome.

4. Detection of "root" access on a device

94. The Temu app checks a user's device to see whether it has "root" access, also known as "super user access." When someone has root access to a device, they have the highest privilege level that can be given.

95. More important to this Complaint, when an app like Temu seeks to detect root access, it is an attempt to avoid third-party scrutiny of the app's code. A cybersecurity researcher needs root access on his or her testing device to investigate and evaluate an app's security.

96. Thus, one purpose of an app trying to determine whether a device has root access[40] is to determine whether the app is being used in a "testing" environment. If the app—like Temu—determines that a device has root access, it can surmise that someone is looking into the app's code and therefore needs to hide any behaviors or functions that it does not want discovered.

97. The State has directly encountered this particular security countermeasure tool in the course of its own forensic investigation of the Temu app.

[40] *How to Implement Root Detection in Android Applications?*, IndusFace, https://www.indusface.com/learning/how-to-implement-root-detection-in-android-applications/#:~:text=Security%20researchers%20or%20pen%20testers,app%20and%20a%20remote%20server (last visited June 3, 2025).

5. Searching for "debuggers"

98. Like root access, security researchers—and security features on mobile devices—may employ a "debugger," which is a tool or program that enables researchers to view the application code while it is running. This is a critical tool for identifying malware that might be hidden within an app.[41]

99. Calls in Temu's code include a query Debug.isDebuggerConnected(), which would alert the Temu app if a debugger is engaged on a user's device. Like the root access detection discussed above, this is intended to obstruct or obscure analysis of the app.

6. Code obfuscation

100. Temu employs "code obfuscation," which is "the process of making an application difficult or impossible to decompile or disassemble, and the retrieved application code more difficult for humans to parse."[42]

101. Analysis of multiple versions of the Temu app show that the files, folders, classes, and functions of the Temu app are designed, named, and cross-referenced to each other in a highly complex way that is meant to hamper investigation of the malicious aspects of the app.

102. Further, analysis reveals that many of these obfuscated lines of code overlap with code from the Pinduoduo app, which has been imported wholesale in multiple instances to the Temu app.

7. Heavily-encrypted network traffic

103. The Temu app must send and receive information over the Internet in order to function on a consumer's device. This information is transmitted in what are colloquially known as "packets," and the sending and receiving of packets is known as "network traffic."

104. Ordinarily, apps protect information and data network traffic using a system called Transport Layer Security (TLS), which encrypts the data in such a way that it can be decrypted,

---

[41] Srinivas, *Debugging for malware analysis*, Infosec (Aug. 14, 2019), https://www.infosecinstitute.com/resources/malware-analysis/debugging-for-malware-analysis/.

[42] *What is code obfuscation and how does it work?*, Guardsquare, https://www.guardsquare.com/what-is-code-obfuscation (last visited June 3, 2025).

read and understood by the user's device and the server communicating with the device, but cannot be decrypted, read, or understood by any other party that may handle or intercept the network traffic.

105. TLS is one pillar on which the modern Internet is built and is so secure that it is regularly relied on to protect the most sensitive types of personal information transmitted digitally, including financial and banking information and federally protected health information while that information is in transmission between a secure server and a user's device.

106. Even apps that deal with the most sensitive types of user data usually do not apply additional layers of encryption beyond TLS to data that is being transmitted between a user's device and the app's servers.

107. The Temu app, on the other hand, uses at least three layers of encryption beyond ordinary TLS to obfuscate data that the app transmits from a user's device to Temu's servers. This method of encrypting data applies the same encryption algorithm at least four times in succession and essentially layers four distinct levels of encryption nested within each other like Russian dolls. When one layer of the encryption is decrypted, it contains some readable data and additional data that is further encrypted and requires a different passkey to decrypt.

108. Critically, this multi-level encryption makes it exceedingly difficult—and at times, entirely impossible—to see the precise data or even *types* of data that are being transmitted to and from the Temu app. In turn, this makes it easier for Temu to send surreptitiously-acquired PII from a user's device without being caught.

109. The State's technical analysis has been able to decrypt some (but not all) of the layers of encryption the app applies to the data it transmits to Temu servers. The State's investigation discovered that some deeper layers of encrypted data transmitted to Temu's servers by the app contains information about the device that is never disclosed to the user, including specific information about the user, the device, and the way the user interacts with the device outside of the Temu app.

///

///

ii. Overlap with Pinduoduo Code

110. Analysis of the code of both the Pinduoduo app and the Temu app show that the latter imports large swaths of code from the former, wholesale. Initial review provides the following examples:

1. Package name overlap

111. Multiple packages of code within the Temu app are lifted wholesale from Pinduoduo. Conceptually, a "package" is a way of organizing related code, much like the folders on one's computer that are used to keep files organized. And, like files on one's computer, packages must be named. Multiple packages in the Temu app begin with the naming convention "com.xunmeng.pinduoduo," and are proprietary, non-public packages, meaning that they were developed by PDD and were copied wholesale from the Pinduoduo app and pasted into Temu.

2. Specific code overlap

112. Analysis reveals that thousands of lines of code overlap between Pinduoduo and Temu. It bears noting that in the Temu code, package names containing the overlapping code often are obfuscated, while in Pinduoduo, they are not. This likely is in an effort to hide the fact that Temu contains Pinduoduo code.

113. The code that overlaps between Temu and Pinduoduo is not benign. For example, both Pinduoduo and Temu contain identical lines of code in the following classes, which in turn deal with the following functionality:

- PhoneInfoManager – the code in this class deals with device identifier collection—including IMEI and MAC Address. The precise data points collected, and the privacy-invasive impact of that collection, are discussed below.
- StorageUtils – the code in this class involves methods for access to user files on their mobile device.
- SecureNative – this code involves custom encryption (i.e., obscuring the two apps' activities).

- ZipPatch – this code is a native library that allows each app to update their respective code without requiring a publishing of the update to the Apple store or Google Play, or with the knowledge or consent of users.

3. SDK overlap

114. SDKs—otherwise known as Software Development Kits—are distinct libraries of code meant to perform specific functions. For example, some SDKs handle identifying and compiling statistics about app performance, others serve targeted ads, and others render graphics in an app. Temu and Pinduoduo have always had an overlap of multiple SDKs, with an overlap of 34 separate and distinct SDKs at their historical peak. One of the most pernicious overlaps of SDKs is the Manwe SDK, discussed above.

iii. Excessive, Unjustifiable, and Hidden Collection of Users' PII

115. As discussed above, much of Temu's efforts to hide its behavior are done in furtherance of accessing and controlling virtually all aspects of a user's device, and surreptitiously acquiring the sensitive PII contained therein.

1. Users' granular location data

116. The State's analysis reveals that the Temu app gains access to user's "fine" location—that is, the app gets user's real-time GPS location within an accuracy of at least 10 feet. As discussed above, Temu removed the permission, ACCESS_FINE_LOCATION, from the Temu app's Android manifest for a period of time in 2023, only to add the permission back to the app once Temu had been called out for this conduct, demonstrating an intent to keep this functionality hidden from the public.

117. At all times, including while the ACCESS_FINE_LOCATION permission was removed from the app manifest, the Temu app continually acquired data points from users that allowed Temu to determine users' precise location regardless of whether the app formally included the ACCESS_FINE_LOCATION permission. However, by removing the ACCESS_FINE_LOCATION permission from the Android manifest, Temu concealed the fact that it was obtaining the precise location of app users in a different, more concealed way.

///

118. Many of the data points Temu continued to acquire and which allowed it to determine precise location without formally including the ACCESS_FINE_LOCATION permission are discussed below in paragraphs 119 through 121 and 139 through 143.

2. WiFi access points

119. The Temu app contains the permission ACCESS_WIFI_STATE, which enables it to collect the name and signal strength of WiFi networks utilized by the individual's device, as well as all WiFi networks that are near a user's device, whether or not the device is connected to those networks.

120. Collecting these data points over time enables the Temu app to create a detailed map of a user's travels throughout the day. When aggregated, these data points provide a detailed map of any place that Temu users have been, whether or not those users ever consented to providing geolocation data.

121. This type of data already has been used to create this kind of global mapping. Recently, the company Niantic announced that it would be building a "Large Geospatial Model" (LGM) that combines millions of scans taken from the smartphones of players of its popular app, Pokémon Go. As explained by Niantic's chief scientist, "Using the data our users upload when playing [our] games . . . we built high-fidelity 3D maps of the world, which include both 3D geometry (or the shape of things) and semantic understanding (what stuff in the map is, such as the ground, sky, trees, etc)."[43]

3. Microphone and camera access

122. Two permissions that Temu includes in its app are requests for CAMERA and RECORD_AUDIO, surreptitiously granting the app access to all of the audio and visual recording and storage functions of a user's device. These permissions are not adequately disclosed to users, as described in paragraphs 141 through 147 below.

[43] Wes Davis, *Niantic is building a 'geospatial' AI model based on Pokémon Go player data*, The Verge (Nov. 19, 2024, 8:07 PM), https://www.theverge.com/2024/11/19/24300975/niantic-pokemon-go-data-large-geospatial-model.

4. Intentional Android exploit: ActivityManager.getRunningTasks

123. The Temu app code contains the method ActivityManager.getRunningTasks. This method was actually deprecated by Android over a decade ago, with the release of Android 5.0 (Lollipop) on November 4, 2014. This was because of its ability to be exploited by developers seeking to acquire a user's personal information, largely in the form of being able to view a user's app usage patterns across their entire device (i.e., it enables Temu to view activity of *all* running apps on a user's phone, and not just activity related to the Temu app).[44]

124. What is particularly concerning about the inclusion of this method within Temu's code is that, as explained above, it was deprecated over a decade ago,[45] in November 2014. Because Temu was not founded until 2022, this means that there was *never* a benign reason for Temu to include this method in its code. Instead—and consistent with Defendants' employment of 100 engineers and product managers to identify and incorporate Android exploits into the Temu and Pinduoduo apps—the only reason to include this method is in furtherance of a purposeful and opportunistic exploit of users who have devices running older operating systems.

125. This analogizes to a thief walking down the street and trying the door of every car and house to see if they are locked. In most instances, they will be, but in the rare event that a door is not locked (meaning a user is using an older device with an older operating system, as would be common in certain populations like elderly users), the thief can take advantage of this security lapse and take whatever they wish from inside.

126. Additionally, the use of ActivityManager.getRunningTasks allows Temu to collect runtime metadata from files on a device like "proc/self/maps," "proc/self/cmdline," and "proc/self/environ," which is a common technique to detect debuggers. *See* ¶¶ 98–99, *supra*.

[44] Shubham Panchal, *Accessing App Usage History in Android*, droidcon (Feb. 8, 2022), https://www.droidcon.com/2022/02/08/accessing-app-usage-history-in-android/.

[45] In the context of software development, "deprecated" refers to a feature, function, or method that is considered outdated or no longer recommended for use but is still supported. While it still functions, its use is discouraged because newer, more efficient, or secure alternatives are available.

5. Intentional Android exploit: android.telephony.TelephonyManager.listen()

127. Android Developer documentation explains that the method android.telephony.TelephonyManager.listen() "[p]rovides access to information about the telephony services on the device. Applications can use [these methods] to determine telephony services and states, as well as to access some types of subscriber information. Applications can also register a listener to receive notification of telephony state changes."[46]

128. Telephony information, broadly, includes information about the telephony services such as subscriber ID, SIM serial number, phone network type, and phone state (status of ongoing calls, phone number, etc.).

129. Critically, *both* android.telephony.TelephonyManager.listen() and ActivityManager.getRunningTasks have been identified as prima facie evidence of malware in at least one recent paper on digital security, which states:

> "android.telephony.TelephonyManager.listen() and android.app.ActivityManager.getRunningTasks() are sensitive APIs that can violate users' privacy" and are identified as useful heuristics when training models to identify malware at scale.[47]

130. The Temu app includes this method, which allows the shopping app to access detailed, private and sensitive information about the user's device, how it connects with their cellular service provider, including incoming and outgoing phone calls.

6. List of all apps installed on user's device

131. Temu contains code that allows it to identify all of the applications installed on a user's device, via the method getPackageManager().getInstalledPackages.

---

[46] Android, *TelephonyManager*, Developers—Guides, https://developer.android.com/reference/android/telephony/TelephonyManager (Apr. 17, 2025).

[47] Lingru Cai et al., *JOWMDroid: Android malware detection based on feature weighting with joint optimization of weight-mapping and classifier parameters*, 100 Comput. & Sec. 1012086 (2021).

132. Such behavior violates the "sandbox" established by both Apple and Google for their respective operating systems (iOS and Android). "Sandboxing" is a principle that keeps one app from gathering data about other apps on a user's device. This privacy-protective principle is self-explanatory: no one app has any need for—nor any business in obtaining—information about the other apps on an individual's device.

133. Additionally, Temu utilizes "query" commands, which seek information about various aspects of a user's device. Initially, Temu utilized broad terms, enabling it to get an exhaustive list of the installed applications on a user's device.

134. The State's analysis revealed that such queries would return data that includes, but is not limited to: (1) the name of every installed app on a user's device; (2) likely install and update timestamps; (3) the version of the installed app; and (4) unknown flags and IDs for each entry.[48]

135. More recently, in response to efforts by Android to prevent this kind of behavior—that is, preventing one app from getting an exhaustive list of other apps on a user's device without the user's notice or consent—Temu has reigned in its queries to address specific apps. However, the queries still search for a wide array of specific apps across a continuum of categories. These apps and categories include, but are not limited to:

- Social Media and Messaging: WhatsApp, Facebook, Instagram, Snapchat, Signal, Telegram, Line, and Discord.
- Financial and Payment Apps: PayPal, Klarna, AfterPay, MobilePay, Toss, Swish, and Satispay.
- Miscellaneous: Google Play Store, Google Maps, and the Samsung Galaxy Store.

[48] As explained in paragraphs 55–56, *supra*, the purpose of this data collection was done by Defendants in order "to spy on users and competitors, allegedly to boost sales."

7. List of all of the accounts a user has stored on the phone

136. Forensic analysis also reveals that the Temu app has contained, at different points in time, the GET_ACCOUNTS permission. Per Android, this permission "[a]llows access to the list of accounts in the Accounts Service."[49]

137. The Android developer guidance further explains that this means an app with this permission gets access to the device's AccountManager code, which "provides access to a centralized registry of the user's online accounts."[50]

138. Virtually everyone that has a smart device also has scores of apps that require an account: social media, dating, banking, health, email, travel, mental wellbeing, exercise, entertainment—the list is practically infinite. Temu does not disclose to its users that it accesses the centralized registry of these online accounts.

8. Additional sensitive PII

139. Temu also collects a host of other discrete PII generated by the user's device, which is universally recognized as individually-identifying pieces of information that can be—and routinely are—used to track, monitor, and profile individuals. That PII includes the items listed in ¶¶ 140–143.

140. **International Mobile Subscriber Identity ("IMSI")**: these are uniquely-identifying data points that are associated with each mobile phone's unique SIM card. They also are instrumental in allowing an individual's device to switch from cell tower to cell tower as the individual moves. This means that if you have an individual's IMSI, you can track that individual without their knowledge or consent.

141. **Media Access Control ("MAC") Address**: a MAC address is a unique, 12-digit hexadecimal number assigned to a specific device (for example, e0:6c:4f:8b:aa:d7). A MAC address uniquely identifies a user's device to each network it connects to. Therefore, like the IMSI discussed above, MAC addresses are used to track an individual's location as they move

[49] Android, *Manifest.permission*, Developers—Guides, https://developer.android.com/reference/android/Manifest.permission#GET_ACCOUNTS (Mar. 13, 2025).

[50] Android, *AccountManager*, Developers—Guides, https://developer.android.com/reference/android/accounts/AccountManager (Feb. 13, 2025).

from WiFi network to WiFi network. For example, documents released by NSA whistleblower Edward Snowden show that the Canadian spying agency CSEC illegally used MAC addresses collected from passengers at a major Canadian airport to track the wireless devices of thousands of ordinary airline passengers for days after they left the terminal.

142. **International Mobile Equipment Identity ("IMEI")**: like the other data elements described in this section, an IMEI is a unique identifier that is associated with a given individual's device. And, just like the above-identified PII, an IMEI can be used to identify a specific individual's location over time, along with that individual's usage of his or her device, more generally. Beyond unauthorized tracking, an IMEI can be used to clone an individual's device, leading to identity theft and other fraud.[51]

143. **Android Advertising ID ("AAID")**: this is a unique identifier used to track an individual's activity over time and across the various apps or websites he or she engages with. As the name suggests, it is used for advertising purposes—that is, data profilers will use this PII to record an individual's activity, and then draw inferences about the person based on that information (ostensibly in hopes of serving targeted ads to the person that are likely to result in a sale).

E. Users Do Not Consent to Defendants' Data Collection Practices.

144. Temu not only seeks a breathtaking array of sensitive data—well beyond what would be necessary or even justifiable for an e-commerce app—but does so in a way that is purposely secretive and intentionally designed to avoid detection.

145. This is all the more egregious given that Defendants have issued recent statements to the press in response to online commenters complaining about Temu's data practices,

[51] Kpurvii, *Should You Keep Your IMEI Number Hidden for Enhanced Mobile Security?*, Device Safety (Dec. 22, 2023), https://devicesafety.org/should-you-keep-your-imei-number-hidden-for-enhanced-mobile-security/.

declaring: "At Temu, we prioritize the protection of privacy and are transparent about our data practices."[52]

146. But this is not true. Defendants cannot be said to apprise their users of their conduct. Indeed, Defendants have designed Temu to have secretive and obfuscated code and functions meant to expressly *hide* their conduct from users.

147. This has been demonstrated time and again, in multiple contexts separate and apart from this litigation. Two of the most obvious examples: Pinduoduo and Temu were pulled from Google's and Apple's app stores, respectively, for failure to disclose to their users the full extent of data being collected. *See* ¶ 10, *supra*.

148. Temu's own disclosures to its consumers only confirm its intent to hide its conduct and cannot be said to establish consent on the part of their users. A survey of the operative Privacy Policies in effect from October 17, 2022 through the present show that Temu has kept the conduct challenged in this Complaint hidden from its users.

October 17, 2022[53]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 122)	No mention of seeking microphone access (or of audio, generally)
Camera Access (¶ 122)	Temu states that it only acquires photos provided by the user, in the course of using the Temu platform: "Personal Information We Collect … Information You Provide to Us. Personal information you may provide to us through the Service or otherwise includes: …

[52] Esme Murphy & Liz Christy, *Talking Points: Are Temu and Shein's fashion deals too good to be true?*, CBS News (Nov. 8, 2023, 6:18 PM), https://www.cbsnews.com/minnesota/news/talking-points-too-good-to-be-true-deals-on-temu-and-shein/; *see also*, Chantelle Francis, *Millions of Aussies shopping on Temu warned as popular Chinese retailer under scrutiny*, The Chronicle (Apr. 9, 2024, 11:59 AM), https://www.thechronicle.com.au/technology/online/millions-of-aussies-shopping-on-temu-warned-as-popular-chinese-retailer-under-scrutiny/news-story/56af0985badb2506df84f280c0c3a63f.

[53] *Privacy & Cookie Policy*, Temu (Oct. 17, 2022), https://web.archive.org/web/20221127065309/https:/www.temu.com/privacy-and-cookie-policy.html.

	User-generated content, such as profile pictures, photos, images, videos, comments, questions, messages, and other content or information that you generate, transmit, or otherwise make available on the Service, as well as associated metadata."
Location Data (¶¶ 89–92, 116–121, 138–142)	Temu states that it only collects location data through device data (which it states can only identify "general location") or when a user provides authorization: "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…general location information such as city, state or geographic area. … Location data when you authorize the Temu mobile app to access your device's location."
WiFi Access Points (¶¶ 119–121)	No mention of WiFi Access Points. The only time "Wi-Fi" appears in the document is under "Automatic data collection…Device data," when Temu states that it collects "radio/network information (e.g., Wi-Fi, LTE, 3G)".
User's Activity on His or Her Device, Outside of Temu (¶¶ 123–126; 130–137)	The only mention of acquiring user data from his or her activity outside of the Temu platform is as follows: "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Online activity data, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them."
Phone State/Telephony (¶¶ 127–129)	Temu's privacy policies make no mention that the app collects this type of data.

List of non-Temu apps or accounts installed on a us device (¶¶ 130–137)	There is no mention of Temu's collection of all installed apps or accounts on a user's device, nor of the app-specific queries that Temu runs.
IMSI, MAC Address, IMEI, AAID (¶¶ 138–142)	Temu states only that it collects "unique identifiers (including identifiers used for advertising purposes)," and does not explain either the specific identifiers it collects, nor does it disclose their sensitivity or their ability to be used to discern location information. "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…unique identifiers (including identifiers used for advertising purposes)[.]"

February 13, 2023[54]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 122)	No mention of seeking microphone access (or of audio, generally), with the exception of a notice at the end of the document titled "Information for California Residents…Right to correction…In the last 12 months, we've collected the following categories of personal information…Audio, electronic, visual, or similar information."
Camera Access (¶ 122)	Temu states that it only acquires photos provided by the user, in the course of using the Temu platform: "Personal Information We Collect … Information You Provide to Us. Personal information you may provide to us through the Service or otherwise includes: … User-generated content, such as profile pictures, photos, images, videos, comments, questions, messages, and other content or information that you generate, transmit, or otherwise make available on the Service, as well as associated metadata."

[54] *Privacy & Cookie Policy*, Temu (Feb. 13, 2023), https://web.archive.org/web/20230314181236/https:/www.temu.com/privacy-and-cookie-policy.html.

Location Data (¶¶ 89–92, 116121, 138–142)	Temu states that it only collects location data through device data (which it states can only identify "general location") or when a user provides authorization: "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…general location information such as city, state or geographic area. … Location data when you authorize the Temu mobile app to access your device's location."
WiFi Access Points (¶¶ 119–121)	No mention of WiFi Access Points. The only time "Wi-Fi" appears in the document is under "Automatic data collection…Device data," when Temu states that it collects "radio/network information (e.g., Wi-Fi, LTE, 3G)".
User's Activity on His or Her Device, Outside of Temu (¶¶ 123–126; 130–137)	The only mention of acquiring user data from his or her activity outside of the Temu platform is as follows: "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Online activity data, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them."
Phone State/Telephony (¶¶ 127–129)	Temu's privacy policies make no mention that the app collects this type of data.
List of non-Temu apps or user accounts installed on a user's device (¶¶ 130–137)	There is no mention of Temu's collection of all installed apps or accounts on a user's device, nor of the app-specific queries that Temu runs.

IMSI, MAC Address, IMEI, and AAID (¶¶ 138–142)	Temu states only that it collects "unique identifiers (including identifiers used for advertising purposes)," and does not explain either the specific identifiers it collects, nor does it disclose their sensitivity or their ability to be used to discern location information. "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…unique identifiers (including identifiers used for advertising purposes)[.]"

149. In the February 2023 Privacy Policy, Temu separately mentions a "Privacy Notice Addendum to US Residents," but the text of that document does not appear in this Privacy Policy. Instead, Temu describes the document as follows:

> **Privacy Notice Addendum for US Residents**
> Residents of certain US states may have additional privacy rights under applicable state privacy laws. US users can learn more about which rights may be available to them and how to exercise those rights by reviewing US Privacy Notice Addendum for US Residents.

150. Temu phrases this as alerting "[r]esidents of certain US states" (Temu does not specify which), that they may have additional *rights*. It does not indicate that it would disclose *more data that it would collect*. This cannot be construed as a disclosure for any purpose, and nothing in the Privacy Policy would put a reader on notice that they should read the Addendum for a more transparent list of PII that Temu collects. But ultimately, this is irrelevant, as nothing in the Addendum could be said to remedy the defects in Temu's Privacy Policy.

///

///

///

///

May 12, 2025[55]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 122)	No mention of seeking microphone access (or of audio, generally), with the exception of a discussion about customer service: "Customer Support Activity When you communicate with our customer service team through our customer support functions in the mobile application/on the website, either with a customer service agent or with our virtual assistant (via the chatbot or hotline), through social media, or any other means, we will collect your communication history with us which includes any text, images, video, audio, or supporting documents exchanged between us."
Camera Access (¶ 122)	Temu removed its prior language quoted above and now says the following: "What Information Do We Collect … User-generated content When you provide product reviews and ratings on the Service, we collect this information, including any accompanying images, videos or text, as well as associated metadata."
Location Data (¶¶ 89–92, 116–121, 138–142)	Temu removed its prior language quoted above and now states as follows, regarding location: "What Information Do We Collect … General location data We collect your approximate location based on your technical information (e.g., IP address)."
WiFi Access Points (¶¶ 119–121)	Temu removed its prior language quoted above and has not provided substitute language.
User's Activity on His or Her Device, Outside of Temu (¶¶ 123–126; 130–137)	Temu removed its prior language quoted above and now states: "Information collected automatically

[55] *Privacy Policy*, Temu (May 12, 2025), https://www.temu.com/ie/privacy-and-cookie-policy.html.

	To enhance your experience with the Service and support the other purposes for which we collect Personal Data as outlined in this Privacy Policy, we automatically process information about you, your computer or mobile device, your interactions with the Service, and our communications over time, such as: … Device data We collect Personal Data about the device you use to access the Service, such as device model, operating system information, language settings, unique identifiers (including identifiers used for advertising purposes where we have a legal basis for doing so). … Service usage information We collect Personal Data about your interactions with the Service, including the items in your shopping cart, your order pages you view, your duration on a page, the source from which you arrived at a page, your interactions with a page, your searched text and images, your browsing history, whether you opened our emails, and whether you clicked the links within our emails. We also collect service-related, diagnostic, and performance information, including crash reports and performance logs."
Phone State/Telephony (¶¶ 127–129)	Temu's privacy policies make no mention that the app collects this type of data.
List of non-Temu apps or user accounts installed on a user's device (¶¶ 130–137)	There is no mention of Temu's collection of all installed apps or accounts on a user's device, nor of the app-specific queries that Temu runs.
IMSI, MAC Address, IMEI, and AAID (¶¶ 138–142)	Temu now states that it collects "unique identifiers (including identifiers used for advertising purposes where we have a legal basis for doing so)," and does not explain either the specific identifiers it collects, nor does it disclose their sensitivity or their ability to be used to discern location information.

///

///

///

///

F. Defendants Are Violating Plaintiffs' Right to Privacy of Their Data

151. As the immediately foregoing sections make clear, Temu (1) collects a host of privacy-invasive PII and (2) it purposely designed its app *and* its customer disclosure in a way to keep its conduct hidden.

152. As a result, Arizonans have incurred, and continue to incur, harm as a result of the invasion of privacy stemming from Defendants' deceptive and unfair acquisition and possession of their PII.

153. Arizonans have a reasonable expectation of privacy in the PII contained on their mobile devices, as well as in their autonomy interests of the mobile devices themselves.

154. "Invasion of privacy has been recognized as a common law tort for over a century." *See Matera v. Google Inc*., No. 15-CV-0402, 2016 WL 5339806, at *10 (N.D. Cal., Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A–I for the proposition that "the right to privacy was first accepted by an American court in 1905, and 'a right to privacy is now recognized in the great majority of the American jurisdictions that have considered the question'"); *see also,* Restatement (Second) of Torts § 652B (Am. Law. Inst. 1977) (defining an "Intrusion upon Seclusion" claim as: "One who intentionally intrudes, physically or otherwise, upon the solicitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

155. As Justice Brandeis explained in his seminal article, *The Right to Privacy*, "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890). The Supreme Court similarly recognized the primacy of privacy rights, explaining that the Constitution operates in the shadow of a "right of privacy older than the Bill of Rights[.]" *Griswold v. Conn.*, 381 U.S. 479, 486 (1965).

156. More recently, the Supreme Court explicitly recognized the reasonable expectation of privacy an individual has in his or her cell phone, and the PII generated therefrom,

in its opinion in *Carpenter v. U.S.*, 585 U.S. 296 (2018). There, the Court held that continued access of an individual's cell phone location data constituted a search under the Fourth Amendment because "a cell phone—almost a 'feature of human anatomy[]'—tracks nearly exactly the movements of its owner . . . A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales . . . Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 311–12 (internal citations omitted).

157. And, even more recently, the Northern District of California, in an order denying a motion to dismiss an intrusion upon seclusion claim for the exfiltration of PII in different mobile apps, held that "current privacy expectations are developing, to say the least, with respect to a key issue raised in these cases—whether the data subject owns and controls his or her personal information, and whether a commercial entity that secretly harvests it commits a highly offensive or egregious act." *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1035 (N.D. Cal. 2019). The *McDonald* court's reasoning was subsequently adopted in the District of New Mexico in analogous litigation. *See New Mexico ex rel. Balderas v. Tiny Lab Prods*., 457 F. Supp. 3d 1103, 1127 (D.N.M. 2020), *on reconsideration*, *New Mexico ex rel. Balderas v. Tiny Lab Prods*., 516 F. Supp. 3d 1293 (D.N.M. 2021).

158. It is precisely because of Defendants' capacity for "near perfect surveillance" that courts have consistently held that time-honored legal principles recognizing a right to privacy in one's affairs naturally apply to online monitoring. Defendants' unlawful intrusion into their users' privacy is made even more egregious and offensive by the fact that the Defendants are targeting and collecting information in a manner that is *intended to go undetected*.

159. As discussed above, Defendants have designed the Temu app to collect a wide range of data from Temu users. In addition, Defendants continue to take actions and have purposefully designed the Temu app to obscure and hide their unlawful collection of users' data.

///

///

160. Defendants' actions also adversely impact non-users of Temu who have had electronic communications with Temu users or whose data is stored on the device of a Temu user because their data is subject to harvesting by Defendants without their knowledge.

161. Many of the categories of data and information collected by Defendants are particularly sensitive. As just one example, Defendants collect physical and digital location tracking data that is highly invasive of Temu users' privacy rights. "Location data is among the most sensitive personal information that a user can share with a company . . . . Today, modern smartphones can reveal location data beyond a mere street address. The technology is sophisticated enough to identify on which floor of a building the device is located."[56] Over time, location data reveals private living patterns of Temu users, including where they work, where they reside, where they go to school, and when they are at each of these locations. Location data, either standing alone, or combined with other information, exposes deeply private and personal information about Temu users' health, religion, politics and intimate relationships. More generally, the various functions and aspects of the Temu app described above make clear that it is a malicious app designed to covertly harvest user data in violation of their privacy rights.

G. Defendants Have Collected Personal Information from Minors, Including Minors Under the Age of Thirteen

162. As described above, Temu surreptitiously collects vast quantities of PII from its users, without their knowledge or consent. These practices are particularly abusive, given that many of the users of Temu are minors, including minors under the age of thirteen. At all relevant times, Defendants have been aware that minors, including minors under the age of thirteen, are using the Temu platform.

163. Nonetheless, Defendants failed to take adequate measures to protect minor users from these abusive tactics or to ensure that minor users, including minor users under the age of thirteen, had parental consent before they used the Temu platform. Nor did Defendants implement adequate age verification procedures or procedures to confirm that minor users were

[56] Christopher Cole, *Sens. Prod Zuckerberg: Why Keep Tracking User Locations?*, Law360 (Nov. 19, 2019, 9:07 PM), https://www.law360.com/consumerprotection/articles/1221312.

acting with the consent of their parents in using the Temu platform or adequate opt-out rights or rights to delete collected information.

164. Anyone can use Temu without verifying his or her age, and indeed many children use the Temu platform, including children under thirteen years old. Temu sells a wide variety of products that are marketed to children such as children's toys and clothing. Defendants have increased their revenue and profits by marketing these products to minors and by collecting minors' personal data when minors accessed the Temu platform.

165. Many of the advertisements for products on Temu are directed toward children, sometimes in inappropriate ways. For example, the United Kingdom's Advertising Standards Authorities recently found that certain Temu advertisements inappropriately sexualized children.[57] Likewise, a consumer group in the United Kingdom found that Temu was selling age-restricted weapons such as survival knives and axes that were illegal for children to possess without any age verification.[58] Others have observed that Temu is filled with smoking and drug paraphernalia that is sold to any customer, without age verification.

166. Finally, Temu recently ran an advertisement multiple times during the 2024 Super Bowl that featured a young-looking animated cartoon protagonist in an animated cartoon world who uses magic to bestow low-priced Temu products on everyone she encounters. (See Figure 3) Attorneys General from several states as well as members of Congress urged CBS not to run the ad given ongoing investigations by Congress into Temu, and the company's documented relationship with the Chinese Communist Party. As one congresswoman who objected to the advertisement observed, it "looked like it belonged on a children's show."[59]

---

[57] *Adverts for online shopping platform Temu banned for sexualising a child and objectifying women*, Sky News (Nov. 1, 2023, 10:51 AM), https://news.sky.com/story/adverts-for-online-shopping-platform-temu-banned-for-sexualising-a-child-and-objectifying-women-12997811.

[58] Sarah Marsh, *Weapons banned in UK apparently found on shopping app Temu*, The Guardian (Nov. 16, 2023, 7:01 PM), https://www.theguardian.com/money/2023/nov/17/weapons-banned-in-uk-apparently-found-on-shopping-app-temu-which.

[59] *Temu's ad controversy: Here's what you need to know*, CNBC (Feb. 12, 2024, 11:46 AM), https://www.cnbc.com/video/2024/02/12/temus-ad-controversy-heres-what-you-need-to-know.html.

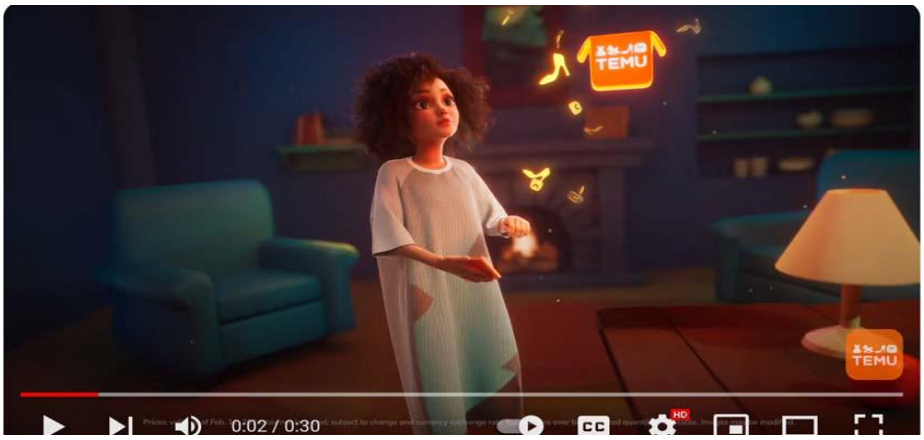

Figure 3: Screen capture of Temu's 2024 Super Bowl commercial.

167. Thus, notwithstanding Temu's statement in its terms of service that "[children] under 13 years are not permitted to use Temu or the Services,"[60] Defendants possess actual knowledge that children under the age of 13 are on the Temu app—and indeed, Defendants actively seek out this audience. Yet Defendants also indiscriminately and surreptitiously mine those children's PII, without providing notice to parents of those children, and without obtaining the parents' verifiable consent.

168. Temu's data collection procedures with respect to minors have also been a specific concern of government authorities. For example, in their ongoing investigation of Temu, members of Congress recently sent a letter to Defendants specifically requesting information regarding Temu's data collection practices with respect to minors.[61]

169. Children under the age of 13 are particularly vulnerable to the harms caused by Defendants' conduct complained of herein, and Defendants' conduct violates longstanding societal norms meant to protect children, and to preserve parents' autonomy to ensure the same.

H. Temu Subjects User Data to Misappropriation by Chinese Authorities

170. While the mere act of invading users' privacy, in the manner described above, is enough to sustain the State's claims without any further allegations, there are additional,

[60] *Terms of Use*, Temu (February 26, 2025), https://www.temu.com/cz-en/terms-of-use.html.

[61] *See* Letter from Cathy McMorris Rogers & Gus M. Bilirakis to Qin Sun, *supra* note 8, at 3

egregious privacy harms that Arizonans have suffered at the hands of Defendants. Namely, Temu's parent is a China-based company that is subject to Chinese law that requires companies to provide user data—including Arizonan's data in Defendants' possession—to the government upon request.

171. Chinese law requires Chinese citizens, and individuals and entities in China to cooperate with national intelligence work undertaken by the Chinese government, and grants regulators broad authority to access private networks, communication systems, and facilities to conduct invasive inspections and reviews.

172. These laws are broad, open-ended, and inscrutably applied. Moreover, there is no independent judiciary in China that operates outside the control of the Chinese Communist Party. Thus, there is no meaningful mechanism in China to resist these demands.

173. Laws including, but not limited to, the National Security Law, Cybersecurity Law, and National Intelligence Law are part of "an interrelated package of national security, cyberspace, and law enforcement legislation" that "are aimed at strengthening the legal basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them."[62]

[62] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017, 11:30 AM), https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense (referring to laws addressing "Counterespionage (2014), National Security (2015), Counterterrorism (2015), Cybersecurity (2016), and Foreign NGO Management (2016), as well as the Ninth Amendment to the PRC Criminal Law (2015), the Management Methods for Lawyers and Law Firms (both 2016), and the pending draft Encryption Law and draft Standardization Law"); *see also* Matt Haldane, *What China's new data laws are and their impact on Big Tech*, South China Morning Post (Sept. 2, 2021, 11:30 AM), https://www.scmp.com/tech/policy/article/3147040/what-chinas-new-data-laws-are-and-their-impact-big-tech (describing later enacted Data Security Law and Personal Information Protection Law as being "built on the groundwork laid by the Cybersecurity Law"); William Zheng, *Big data expert takes over as China's new cybersecurity chief*, South China Morning Post (Sept. 27, 2019, 10:15 PM), https://www.scmp.com/news/china/politics/article/3030563/big-data-expert-takes-over-chinas-new-cybersecurity-chief.

174. China's National Security Law places "the responsibility and duty to safeguard national security" on all "*[c]itizens of the People's Republic of China*, all State bodies and armed forces, all political parties and people's organizations, *enterprises*, undertakings, organizations and all other social organizations."[63]

175. The National Intelligence Law expounds on this responsibility, requiring all organizations and Chinese citizens to "cooperate with national intelligence efforts," and permits national intelligence institutions to collect information, question organizations and individuals, and take control of facilities and "communications tools."[64]

176. Specifically, the National Intelligence Law provides that "[a]ll organizations and citizens shall support, assist, and cooperate in national intelligence work in accordance with law, and keep confidential the national intelligence work that it or he knows. . ."[65]

177. Article 14 provides that "[n]ational intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[66]

178. Article 16 provides that these institutions "may enter relevant restricted areas and venues; may learn from and question relevant institutions, organizations, and individuals; and may read or collect relevant files, materials or items."[67]

179. Article 17 provides that "[a]s necessary for their work, the staff of national intelligence work institutions may, in accordance with relevant national provisions, have priority

---

[63] National Security Law of the People's Republic of China (promulgated by the 12th Nat'l People's Congress Standing Comm., July 1, 2015), art. 11, 2015 P.R.C. Laws (China), available at https://stanford.io/3sScPjX (emphasis added).

[64] National Intelligence Law of the People's Republic Of China (promulgated by the 13th Nat'l People's Congress Standing Comm., Apr. 27, 2018), arts. 7, 17, P.R.C. Laws (China), available at https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

[65] *Id.* art. 7.

[66] *Id.* art. 14.

[67] *Id.* art. 16.

use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings . . . ."[68]

180. Against this backdrop are numerous laws and regulations designed to form a comprehensive cybersecurity regime. The "chief engineer at the [Ministry of Public Security's] Cybersecurity Bureau," Guo Qiquan, described the scheme as intended to "cover every district, every ministry, every business and other institution, basically covering the whole society. It will also cover all targets that need [cybersecurity] protection, including all networks, information systems, cloud platforms, the internet of things, control systems, big data and mobile internet."[69]

181. These laws and regulations include, but are not limited to, China's Cybersecurity Law and Data Security Law.

182. "China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime."[70]

183. The Cybersecurity Law applies broadly to, among others, "network operators," which can encompass not only "telecommunications or internet service providers (ISPs)" but also "anyone who uses [information communication and technology] systems."[71]

184. Article 28 of China's Cybersecurity Law requires these "network operators" to cooperate with national intelligence activities, as well as criminal investigations. Specifically, Article 28 provides that, "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[72]

---

[68] *Id.* art. 17.

[69] Zheng, *supra* note 62.

[70] Sam Sacks & Manyi Kathy Li, *How Chinese Cybersecurity Standards Impact Doing Business in China*, Ctr. for Strategic & Int'l Stud. (Aug. 2, 2018), https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[71] *Id.*

[72] Cybersecurity Law of the People's Republic Of China (promulgated by the 12th Nat'l People's Congress Standing Comm., Nov. 7, 2016), art. 28, 2017 P.R.C. Laws (China), available at https://stanford.io/3T5wes8.

185. Article 49 further provides that "network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law."[73]

186. The Cybersecurity Law applies even more stringent requirements and oversight on organizations deemed "critical information infrastructure operators."

187. For example, Article 35 provides that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council."[74]

188. Article 37 further provides:

> [c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.[75]

189. Since the law's enactment, authorities have issued regulations expanding its scope.[76]

---

[73] *Id.* art. 49.
[74] *Id.* art. 35.
[75] *Id.* art. 37.
[76] *See generally* Bob Li, *China Issued New Measures for Cybersecurity Review in 2022*, White & Case LLP (Feb. 8, 2022), https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022; James Gong, *China Updated its Cybersecurity Review Regime*, Bird & Bird (Jan. 13, 2022), https://www.twobirds.com/en/insights/2022/china/china-updated-its-cybersecurity-review-regime.

190. Exactly what type of organization may be designated a "critical information infrastructure operator" is not always clear. However, authorities' use of the applicable procedures indicates that tech companies and platforms could be subject to an invasive cybersecurity review, and that authorities' power to require a company to take any action pursuant to a cybersecurity review—even if justified only after the fact—could have significant consequences for its business.[77]

191. For example, in July 2021, just a few days after the Chinese ride-hailing service Didi raised billions of dollars in a New York IPO, the Cyberspace Administration of China (CAC), a "merged party-state institution listed under the Central Committee of the Chinese Communist Party,"[78] initiated a cybersecurity review of Didi. The CAC further "suspended new user registrations during the review" and ordered the removal of the company's applications from app stores in China.[79] Although the law and related regulations did not explicitly apply to Didi in advance of the review, CAC published a list of proposed new rules applying the cybersecurity review requirements to Didi *after* it began its review.[80] CAC eventually imposed a $1.2 billion fine on the company.[81]

---

[77] *See* Arendse Huld, *Critical Information Infrastructure in China – New Cybersecurity Regulations*, China Briefing (Aug. 30, 2021), https://www.china-briefing.com/news/critical-information-infrastructure-chinas-new-regulations/; Li, *supra* note 76; Gong, *supra* note 76. *See also* M. Shi et al., *Forum: Unpacking the DiDi Decision,* DigiChina (July 22, 2022), https://stanford.io/3T4ZAqM (explaining the results and implications of the cybersecurity review of Chinese ride-hailing company DiDi).

[78] Jamie P. Horsley, *Behind the Façade of China's Cyber Super-Regulator*, DigiChina (Aug. 8, 2022), https://stanford.io/3FPAOYy.

[79] *Id.*; Li, *supra* note 76.

[80] Horsley, *supra* note 78.

[81] *Id.*

192. The Data Security Law applies in China as well as to "data handling activities outside the mainland territory of the PRC [that] harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC."[82]

193. Article 24 provides that "[t]he State is to establish a data security review system and conduct national security reviews for data handling activities that affect or may affect national security."[83]

194. Further, Article 31 applies "[t]he provisions of the Cybersecurity Law [. . .] to the outbound security management of important data collected or produced by critical information infrastructure operators operating within the mainland territory of the PRC[.]"[84]

195. Under the Data Security law, even "a company holding data belonging to a US citizen stored on a Chinese server may not be able to legally hand over that data to the US government without proper approval."[85] More specifically, under Article 36, whether operating critical information infrastructure or not, companies "are prohibited from providing any data *stored* in China, regardless of the data's sensitivity level and whether or not the data was initially *collected* in China, to any foreign judicial or law enforcement agency without the prior approval of the relevant [Chinese Government] authorities."[86]

196. Experts across a variety of fields, including law, national security, and technology agree that Chinese laws require any individuals or entities in China or otherwise subject to Chinese law to cooperate with the Chinese government, including China's intelligence and

---

[82] Data Security Law of the People's Republic Of China (promulgated by the 13th Nat'l People's Congress Standing Comm., June 10, 2021), art. 2, 2021 P.R.C. Laws (China) available at https://stanford.io/3U5iijm.

[83] *Id.* art. 24.

[84] *Id.* art. 31.

[85] Haldane, *supra* note 62.

[86] Ryan D. Junck et. al, *China's New Data Security and Personal Information Protection Laws: What they Mean for Multinational Companies*, Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates (Nov. 3, 2021), https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws; Data Security Law of the People's Republic of China, art. 36.

security services, and that there is no meaningful way to resist these requirements, or any pressure brought to bear by the Party.[87]

197. Further, Chinese law enforcement and intelligence services interpret Chinese law as applying to any data, wherever it is stored, if China has a national security interest in that data. Chinese authorities have forced even refugees from China to hand over data stored outside of China to Chinese authorities under such circumstances, citing Chinese law.

198. In sum, any data stored *or accessed* by individuals or entities subject to Chinese laws, as written and as interpreted and applied by Chinese government officials, is not safe from access by the Chinese government, for any use it deems fit.

199. The geopolitical reality of a dominant e-commerce platform being controlled by an authoritarian regime drastically amplifies the harms—and the stakes—associated with Defendants' deceptive and unfair practices.

---

[87] *See, e.g.*, Klon Kitchen, *The Chinese Threat to Privacy*, Am. Foreign Pol'y Council, May 2021, at 20, 23, https://www.afpc.org/publications/e-journals/The-Future-of-Great-Power-Competition; Will. Knight, *TikTok a Year After Trump's Ban: No Change, but New Threats*, WIRED (July 26, 2021, 7:00 AM), https://www.wired.com/story/tiktok-year-trump-ban-no-change-new-threats/ (quoting K. Frederick, Director of the Tech Policy Center at the Heritage Foundation); Kara Frederick, et al, *Beyond TikTok: Preparing for Future Digital Threats*, War On The Rocks (Aug. 20, 2020), https://warontherocks.com/2020/08/beyond-tiktok-preparing-for-future-digital-threats/; Julian E. Barnes, *White House Official Says Huawei Has Secret Back Door to Extract Data*, N.Y. Times, Feb. 11, 2020, at B3 (quoting former National Security Advisor Robert O'Brien); Arjun Kharpal, *Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice*, CNBC (Mar. 5, 2019, 12:33 AM), https://cnb.cx/3Gmno6T (quoting NYU Professor of Law Emeritus and Director of the U.S.-Asia Law Institute J. Cohen and M. Thorley, postdoctoral research fellow at the University of Exeter with experience building a business in China); Fergus Ryan et al., *TikTok and WeChat: Curating and controlling global information flows*, Austl. Strategic Pol'y Inst. 36 (Sept. 8, 2020), https://www.aspi.org.au/report/tiktok-wechat/; Drew Harwell and Tony Romm, *Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses*, Wash. Post (Nov. 5, 2019), https://wapo.st/3WPMX5S (quoting Alex Stamos, Director of the Stanford Internet Observatory).

I. Defendants Acknowledge That They Risk Being Subject to China's Laws Regarding User's Data in Their Possession

200. None of the above is speculation or hyperbole. In a filing to the SEC on April 28, 2025,[88] Pinduoduo (1) acknowledges that Temu is one of its platforms,[89] and (2) states, in a section titled "Risks Related to Doing Business in China," the following:

a. "A significant portion of our assets and operations is located in China. Accordingly, our business, financial condition, results of operations and prospects may be influenced to a significant degree by political, economic and social conditions in China generally."[90]

b. "Our operations in China are governed by PRC laws and regulations. Our PRC subsidiaries are subject to laws and regulations applicable to foreign investment in China."[91]

c. "We only have contractual control over the Pinduoduo platform. We do not directly own the Pinduoduo platform due to the restrictions on foreign investment in businesses providing value-added telecommunications services in China, including e-commerce services and internet content-related services. This may significantly disrupt our business, subject us to sanctions, compromise enforceability of related contractual arrangements, or have other harmful effects on us."[92]

d. "The PRC governmental authorities have promulgated laws and regulations relating to cybersecurity review. The Data Security Law, the Regulations on the Protection of Critical Information Infrastructure, and the Cybersecurity Review Measures promulgated by the PRC authorities (collectively, the 'Cybersecurity

---

[88] PDD Holdings, Form 20-F Annual Report (2024).
[89] *Id.* at 1 (disclosing that "references in this annual report to [. . .] 'our platforms' are to the Pinduoduo platform and the Temu platform").
[90] *Id.* at 11, 51.
[91] *Id.* at 51.
[92] *Id.* at 52.

Laws') impose cybersecurity review obligations on [. . .] network platform operators that hold the data of more than one million users[.]"[93]

e. "[W]e may…be subject to cybersecurity review obligations if the Cybersecurity Review Office decides to initiate a review against us on the grounds that we are deemed to be an operator engaged in offering network products and services or data processing activities that affect or may affect national security, though our ability to control and assess the likelihood of whether this happens is limited."[94]

J. Defendants Also Engage in Deceptive and Unfair Trade Practices in the Offer and Sale of Products on the Temu App and the Resolution of Consumer Complaints.

201. Defendants actively utilize deceptive and unfair practices in order to maximize the number of users who sign up to use the app, thereby maximizing the amount of data that Defendants can misappropriate. According to one commentator, "TEMU is a notoriously bad actor in its industry. We see rampant user manipulation, chain-letter-like affinity scams to drive signups, and overall, the most aggressive and questionable techniques to manipulate large numbers of people to install the app."[95]

202. Defendants seek to induce users to sign up for the Temu app with the promise of low-cost, high-quality goods manufactured in China. Defendants underscore this aspect of the platform through a variety of gimmicks such as pop-ups with wheels to spin for discounts, tokens to collect, and countdown clocks. (See Figure 4)

---

[93] *Id.* at 8; *see also* Casey Hall & Ariana McLymore, *Retailer Temu's daily US users nearly halve following end of 'de minimus' loophole*, Reuters (June 4, 2025, 10:32 AM), https://www.reuters.com/business/retail-consumer/retailer-temus-daily-us-users-halve-following-end-de-minimis-loophole-2025-06-02/ (estimating Temu's global monthly active users to be 405 million).

[94] PDD Holdings, Form 20-F Annual Report (2024) at 8.

[95] *We believe PDD is a Dying Fraudulent Company and its Shopping App TEMU is Cleverly Hidden Spyware that Poses an Urgent Security Threat to U.S. National Interests*, Grizzly Research (Sept. 6, 2023), https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/.

Figure 4: Examples of pop-ups targeted to Temu users.

203. These gimmicks have been wildly successful: "PDD's TEMU online marketplace is being reported as among the fastest uptaken apps in history."[96]

204. However, Defendants' representations regarding the products sold on the Temu platform are false and serve only to further conceal its scheme to maximize the number of users who sign up to the platform and unwittingly subject their private data to theft by Defendants. For example, while Temu represents that it sells "affordable great products,"[97] there have been numerous complaints regarding the quality of goods sold on the site as well as the service provided by Temu.

205. Temu customers in Arizona have submitted dozens of complaints to the BBB and Arizona Attorney General about Temu over the past three years. The experiences of consumers recounted below are merely concrete (but by no means exhaustive) examples of the countless acts by Temu that constitute violations of the ACFA.

i. Deceptive Representations as to the Quality of Goods

206. The Better Business Bureau alone has received hundreds of complaints in the past year, earning Temu a rating of 2.1 out of 5 stars.[98] Users experience undelivered packages and

---

[96] *Id.*

[97] *About Temu*, Temu (last visited June 6, 2025), https://www.temu.com/about-temu.html.

[98] Nicholas Kaufman, *Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes*, U.S.-China Econ. and Sec. Review Comm'n (Apr. 14, 2023), https://www.uscc.gov/research/shein-temu-and-chinese-e-commerce-data-risks-sourcing-violations-and-trade-loopholes.

poor customer service. Moreover, even when goods are delivered, they are often of low quality, contrary to Temu's marketing and representations.

207. For example, one analysis observed that "TEMU products as shipped often do not resemble the photos."[99] Users frequently receive low-quality, cheaply-made merchandise when the photo on the app indicates that they would receive high-quality goods. Moreover, photos and product descriptions are sometimes simply copied directly from other sellers on sites like Amazon, bearing no relationship to the actual goods being sold.[100] In addition, while Defendants claim that they use "world-class manufacturers" and have "strict policies against counterfeit or unsafe goods,"[101] Temu frequently sells counterfeit, knock-off products in violation of the law. For example, it recently was reported that Temu was selling knockoff Air Jordans on the site and continued to do so even after the issue came to light (more on Temu's sale of unlicensed goods below).[102]

208. **On January 22, 2024**, an Arizona consumer ordered an item described on Temu as a "5-level storage container." When the item arrived on February 21, 2024, the item had only one level of storage. Despite the fact that 4/5ths of the item's promised functionality was missing, Temu refused to replace or refund the item because "the item was shipped according to the order."

209. **In July 2024**, an Arizona consumer ordered an air conditioning unit for approximately $300. When the consumer unboxed the air conditioning unit to have it installed in March 2025, the installation technician realized partway through the installation process that the unit did not include a critical electrical wire connection to connect to a power line. The unit

---

[99] Grizzly Research, *supra* note 95.

[100] Jennifer Ortakales Dawkins, *Temu sellers are now even copying product photos, descriptions, and entire Amazon storefronts, lawsuits allege*, Business Insider (Jul. 11, 2023, 8:26 AM), https://www.businessinsider.com/temu-sellers-are-counterfeiting-amazon-listings-and-storefronts-2023-7.

[101] *Temu's Commitments*, Temu (last visited June 6, 2025), https://www.temu.com/commitments.html.

[102] Jennifer Ortakales *Fake Jordans are all over Temu even after the knockoffs were removed from Shein*, Business Insider (Jun. 16, 2023) (available at https://www.businessinsider.com/shein-and-temu-listed-fake-air-jordans-for-under-50-2023-6)

could not function without that electrical wire connection part, and the part is not available from any source other than as part of the air conditioning unit.

210. Despite the missing critical part, Temu refused to accept a return of the defective product or provide the consumer a full refund because, according to Temu, the consumer only realized that the air conditioning unit was missing the critical part outside of Temu's internal "after-sales service period."

211. **On August 12, 2024**, an Arizona consumer purchased a building block set from Temu. The display pictures of the item clearly advertised the item as a specific set with specific size dimensions, including both metric and standard measurements in the photographs, having specific details, and showing an overhead view with a clear layout and number of pieces in the item. When the item first arrived, the product did not match the measurements, detail, or number of pieces represented in the item pictures.

212. Minutes after receiving the package and realizing that the product did not match the representations in the product listing, the consumer contacted Temu to attempt to return and refund the item. Temu informed the consumer that a return of the product had already been processed, and the product was therefore not eligible for a free return.

ii. Pricing Misrepresentations

213. Temu further engages in a deceptive practice known as "false reference pricing," in which a retailer represents to a prospective customer that a product is on sale at a steep discount—for example by providing two prices that the customer can compare to each other: a former list price or manufacturer's suggested retail price ("MSRP") and a supposedly reduced current price—when in reality the "full price" is inflated, or was never real to begin with, while the "discounted" price is merely the product's regular or market price.

214. Defendants engage in such false reference pricing on Temu. One such example was identified in the social media platform Reddit, regarding the sale of the popular video game "Zelda: Breath of the Wild" or "BOTW." In a post titled "*What's it called when a store sells a product for the standard price but crosses out a marked up one?*" a user noted that Temu was

///

claiming the purportedly discounted price of $40 for the video game was misleading, because the game never actually retailed for the advertised "standard" price of $144.[103] (See Figure 5)

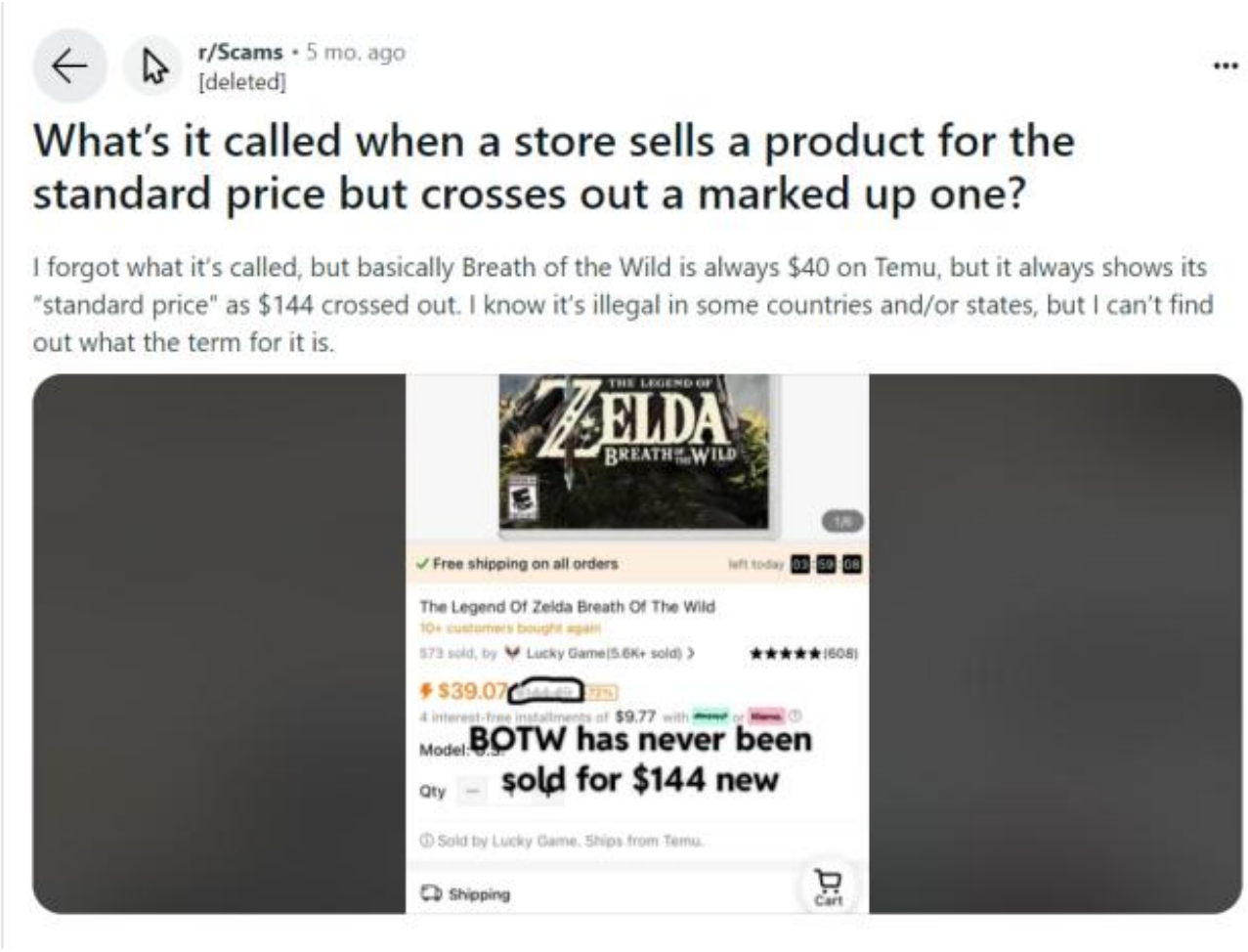

Figure 5: Example of "false reference pricing" on a Temu product listing.

215. **On October 8, 2024**, a consumer purchased two products from Temu with prices of $20.80 each. On October 9, Temu indicated on its website that the products had shipped to the consumer. The next day, a Temu customer service representative called the consumer to claim that the purchased products actually were not in stock, and the consumer would be

[103] IronBrandon22, *What's it called when a store sells a product for the standard price but crosses out a marked up one?*, reddit (Oct. 16, 2023, 11:14 PM), https://www.reddit.com/r/Scams/comments/179oq5y/whats_it_called_when_a_store_sells_a_product_for/.

required to cancel the order to receive a refund. After cancelling the order, the consumer checked the listings for the products and found that the items were in stock and available for purchase, but Temu had increased the price to $32.99 each.

216. **In approximately August 2024**, an Arizona consumer complained that product prices shown on a Temu search page are different than the product price shown on the individual product listing page. The price Temu displayed to the consumer on the search page was lower than the displayed price for the product when the consumer clicked on the product listing. Importantly, none of the prices for the different product options (color, size, or other features) in the listing were as low as the price displayed on the search page. Despite the fact that none of the prices for different product options on the item listing page matched the displayed price on the search page, Temu responded to this complaint by claiming that "The price shown on the listing page is subject to change upon clicking through to the item, as the final price can vary depending on the selected color, size, and other product-specific features."

iii. Charges for Goods Not Ordered or Not Delivered

217. Numerous Arizona consumers have complained to the Better Business Bureau and other consumer watchdog organizations about receiving mysterious packages from Temu that they did not order and Temu charging the consumers for those purchases and other items that they did not order.

218. These fraudulent deliveries and charges occur frequently after consumers make comparatively small purchases from Temu, and then much larger charges and deliveries are made using the same information the consumer provided Temu during checkout for their legitimate purchase.

219. **In approximately May 2025**, an Arizona consumer attempted to purchase a specific guitar from Temu. The consumer completed the purchase transaction, but the seller later contacted the consumer to inform them that the guitar was actually a single unique item and had already been sold to another purchaser. The seller directed the consumer to contact Temu to refund the order, but Temu customer service refused to refund the consumer's purchase, even though the guitar was never delivered.

iv. Use of Forced Labor

220. In addition, while Defendants claim that they seek to "[d]o good for the world," are "honest, ethical and trustworthy," and are "socially responsible,"[104] a recent report found that much of the merchandise sold on Temu is likely being produced using forced labor provided by China's Uyghur minority held against their will in camps in the Chinese province of Xinjiang.[105] As the *Los Angeles Times* noted in a recent exposé, such practices are not only deceptive, but they violate federal law: "Products made in China's western province of Xinjiang are being sold to U.S. consumers through the online shopping platform Temu, in breach of a ban that forbids goods from the region due to links to forced labor, according to research by a global supply chain verification firm." As one expert noted in the article, "It's a systematic violation of U.S. trade policies."[106]

221. As the article explains, "Citing what the U.S. State Department has called 'horrific abuses' against the Uyghur people of Xinjiang, who are predominantly Muslim, federal officials banned the importation of cotton from the region in 2021 and expanded the law and its enforcement to all Xinjiang products last year under the Uyghur Forced Labor Prevention Act. Statements from former detainees and reports from an array of researchers and advocacy groups have alleged that the Chinese government put more than 1 million people in detention camps in the region and that laborers in fields and factories were forced or coerced."[107]

222. The U.S. government has also expressed concerns that Temu is selling Chinese goods to consumers in the United States that are manufactured using forced labor. For example, the Congressional U.S.-China Economic and Security Review Commission issued a report noting that Temu posed "risks and challenges to U.S. regulations, laws and principles of market

---

[104] *About Temu*, Temu (last visited June 6, 2025), https://www.temu.com/about-temu.html.

[105] Sheridan Prasso, *Most-downloaded app in App Store sells products linked to forced labor in China, analysis shows*, L.A. Times (June 15, 2023, 3:21 PM), https://www.latimes.com/business/story/2023-06-15/temu-sells-products-linked-to-forced-labor-in-china.

[106] *Id.*

[107] *Id.*

access" resulting from such direct-to-consumer sales.[108] Likewise, Representative Mike Gallagher, former chair of the House Select Committee on the Chinese Communist Party, and the panel's top Democrat, Raja Krishnamoorthi, who represents Illinois' 8th Congressional district, sent letters to Temu asking for information concerning whether the company is importing products derived from forced labor in China.[109]

223. The House Select Committee on the Chinese Communist Party recently issued an Interim Report regarding its findings to date, entitled "Fast Fashion and the Uyghur Genocide." The report concludes that "Temu does not have any system to ensure compliance with the Uyghur Forced Labor Prevention Act (UFLPA). This all but guarantees that shipments from Temu containing products made with forced labor are entering the United States on a regular basis, in violation of the UFLPA."[110] The report concluded that Temu is actively seeking to avoid the protections in place to prevent the sale of goods manufactured with forced labor: "Temu's business model … is to avoid bearing responsibility for compliance with the UFLPA and other prohibitions on forced labor while relying on tens of thousands of Chinese suppliers to ship goods direct to U.S. consumers."[111] Moreover, the report observed that "Temu admitted that it 'does not expressly prohibit third-party sellers from selling products based on their origin in the Xinjiang Autonomous Region.'"[112]

224. The committee's report was issued after it held hearings at which it received expert testimony regarding the "genocide of the Uyghur people and other minorities." As recounted in the report, "The Committee received first-hand witness testimony and expert reports about the

---

[108] Kaufman, *supra* note 98.

[109] Letter from Mike Gallagher & Raja Krishnamoorthi, United States Congress Select Committee on the Chinese Communist Party, to Mr. Qin Sun, President of Temu (WhaleCo, Inc.) (May 2, 2023) (available at https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-krishnamoorthi-send-letters-forced-labor-concerns-nike-adidas-shein).

[110] Staff of H.R. Select Comm. on the CCP, *supra* note 31, at 2.

[111] *Id.*

[112] *Id.*

CCP's atrocities, which include imprisonment, torture, rape, forced sterilization, and the widespread exploitation of the Uyghur people in forced labor."[113]

225. The committee noted that the hearings provided evidence that Temu ships "millions of packages" to the United States "duty free" and "without providing [U.S. Customs & Border Protection] with sufficient data regarding the contents of the packages[.]"[114] The committee concluded: "In light of the sheer volume of shipments sent to the United States through its website, Temu's failure to take any meaningful steps with respect to preventing the importation of goods produced with forced labor is striking."[115]

226. These unscrupulous practices have allowed Defendants to maximize their access to user data through the false promise of low-cost, high-quality goods. Moreover, they further demonstrate that Defendants' real business is not providing a platform for the sale of quality merchandise but rather obtaining access to user data under false pretenses, which they then misappropriate and seek to monetize.

v. Sign-Up Scams to Lure New Users or to Induce Existing Users to Reel in Their Friends

227. Defendants utilize additional deceptive marketing techniques to induce users to sign up for the platform and grant Defendants access to user data. For example, Defendants run chain letter-like tactics where users are repeatedly urged to sign up their friends and acquaintances in order to expand the number of users whose data Defendants may then access through the app.

228. Among other things, Temu offers credit and free items to users who get their friends and acquaintances to sign up for the app, but "[t]hose who do register are subjected to a bombardment of emails and app notifications."[116] "[O]nce you give TEMU your personal

---

[113] *Id.* at 3.
[114] *Id.* at 7.
[115] *Id.* at 9.
[116] James Titcomb, *Here comes Temu, China's 'scary' bargain-basement Amazon killer*, The Telegraph (Jul. 1, 2023, 12:00 PM), https://web.archive.org/web/20230705172831/

information, you will be repeatedly spammed, hounded, nagged, and bribed to get your friends and family to give TEMU their personal information. When users fall down this rabbit hole (getting that Nintendo Switch absolutely free), TEMU sends a torrent of popup sequences milking users for 'just one more contact'."[117] In addition, Temu users are bombarded by notifications and spam from third parties other than Defendants. These emails and notifications occur even after users delete the app from their devices and even when users seek to block such notifications.

229. Moreover, Temu has utilized online "influencers" to harvest new users on an even larger scale. "There are now literally thousands of so-called 'influencers' hawking TEMU referrals on Reddit, YouTube, TikTok, and also Minecraft, Roblox, Discord [. . .] the pitch is: 'You don't have to buy anything, just sign up!'" "If you have a social media presence, TEMU will figure that out and will start to spam you—every day—to induce you to create videos promoting TEMU, for which they promise to pay."[118]

vi. Fake Reviews

230. Defendants attract and maintain users through other fraudulent means. For example, "TEMU [. . .] compensates users to write reviews," which are then "obviously skewed positive[.]"[119] Moreover, reviews are categorized in a deceptive manner with reviews characterized as "five star" positive reviews when in reality they contain extremely negative comments about the platform. For example, one report cited a so-called "five star" review stating that "What this company is doing is illegal" and constitutes "fraud," that the company relies on "lies and deceptions," and that "[c]ountless reviews are clearly negative, yet it shows that the person gave the item 5 stars which is impossible."[120] Other users have reported that "Some items are legit pretty good, but I've ordered from these sites and most is total crap. I [. . .] wouldn't

---

https://www.telegraph.co.uk/business/2023/07/01/temu-china-bargain-basement-amazon-rival-retail-online-shop/.

[117] Grizzly Research, *supra* note 95.

[118] *Id.*

[119] *Id.*

[120] *Id.*

waste my time if the reviews were more truthful. I've noticed sometimes the text of the review is negative, yet the rating is 5 stars."[121] In response, other users noted that when a user tries to give an item one-star, the rating is automatically "upgraded" to a five-star rating.

231. **In January 2024**, an Arizona consumer reported that Temu falsified product ratings ostensibly from the consumer for products the consumer had previously purchased. When the consumer attempted to write a review of a purchased product, they discovered that Temu had already placed a 5-star rating on the product ostensibly from the consumer, and that the consumer was unable to make changes to the review that had been falsely created in their name.

vii. Gamification, Store Credit and Failure to Honor Terms

232. As illustrated by its gamified nature, Temu is designed to be highly addictive. As one report notes, "[t]he app successfully keeps people hooked. The average user spends around twenty-eight minutes a day on the app, according to Sensor Tower, nearly double the 16 minutes spent on Amazon."[122] The more time users spend on the app, the more data is available for covert collection by Defendants in violation of users' right to privacy in their personal data.

233. Moreover, numerous Arizona consumers have complained that, even when they engage and complete Temu's "games" for promotions, the company fails to provide the promised reward incentives.

234. **In approximately April 2024**, Temu purported to give an Arizona consumer a promotional offer of "10 free items" for being an "excellent customer." The consumer selected ten items and provided payment to ship the items. Temu then charged an additional approximately $209 to the consumer's method of payment for the "free" items. Temu then told the consumer that the items were not returnable. Temu responded to the consumer's complaint by telling the consumer that "this promotion is genuine and was designed to provide our customers with an exciting opportunity to access exclusive deals and discounts."

---

[121] Kennymax123, *Shein, Temu, etc. – What's up with the 5 star reviews for EVERYTHING?!*, reddit (August 10, 2023, 1:21 PM), https://www.reddit.com/r/FrugalFemaleFashion/comments/15niiki/shein_temu_etc_whats_up_with_the_5_star_reviews/.

[122] Titcomb, *supra* note 116.

235. **On April 17, 2024**, a different Arizona consumer downloaded the Temu app and Temu presented the consumer with a promotional offer to receive "6 free gifts and $300 in merchandise" if the consumer made a purchase of at least $20. After the consumer made a purchase of $24.40 as required by the promotional offer, Temu presented additional merchandise available to order the 6 free gifts.

236. After the consumer selected the 6 items to receive the free gift, Temu then informed the consumer that, as an additional requirement to receive the 6 free gifts, the consumer was required to invite other users to join the app via Facebook, Instagram, or text message. The consumer complied with Temu's additional hurdle to receive their promised promotional award by sending the required number of invitations to their contacts.

237. After complying with all of Temu's successive demands to receive the their "6 free gifts," the consumer clicked "submit" on the app. Temu immediately charged the consumer $119.75 for the "6 free gifts" in the consumer's checkout basket.

238. When the consumer complained about Temu's series of misrepresentations, Temu responded that "the rewards issued to [the consumer] are consistent with the activity according to our rules and policies. Unfortunately, we cannot make exceptions to the rules for any individual participant. Please rest assured that the activities are real and valid. Meanwhile, we value your feedback and will continue to optimize the display of the activity page to provide a better user experience."

239. **In approximately July 2024**, an Arizona consumer purchased a shoe rack from Temu that did not work as expected. Temu's website states that return shipping is free for the first time any item is returned. The shoe rack was delivered to the consumer in two separate boxes, but when the consumer attempted to return the shoe rack, Temu provided only one return label. The consumer contacted Temu and a customer service representative named Nino told the consumer to purchase an additional return label and Temu would reimburse the cost of the return label for the second box. When the consumer sent Temu proof of payment for the second return label, Temu informed the consumer that it would not reimburse the consumer directly for the cost of the return label, but would instead offer $12.95 in store credit to the consumer,

effectively forcing the consumer to make an additional $12.95 purchase in order to return the defective shoe rack.

240. **In approximately July 2024**, a different Arizona consumer returned several defective items to Temu, and received $92 in store credit for the returns. When the consumer then attempted to make a separate purchase using the $92 in credit, Temu informed the consumer that it had suspended the consumer's account, and the $92 was unavailable to pay for purchases.

241. **In January 2025**, a different Arizona consumer complained that in order to use the store credits saved in her account from promotions or past returns, Temu required her to purchase an item for a price higher than the amount she had on her account in store credit, pay the full higher price, and Temu then promised to apply the store credits to refund the payment method. Temu therefore required the consumer to spend additional money to access and use the "store credit" that Temu purported to give her through promotions or past returns.

viii. Intellectual Property Theft

242. Temu claims to be "committed to protecting everyone's intellectual property and [to] have a comprehensive policy to that end."[123] But that statement is woefully misleading in light of the actual details of Temu's policy, Temu's procedures for reporting intellectual property violations, and the literally countless products that are available for purchase from the Temu store that infringe on intellectual property rights.[124]

243. For an IP rightsholder to merely request that Temu review an infringing product, the rightsholder is required to create a Temu customer account before gaining access to the Temu Intellectual Property Complaint Portal. To submit a removal request, the rightsholder is then required to enter extensive information about each specific product listing that violates their intellectual property. Notably, Temu commonly generates multiple, sometimes dozens, of separate and independent listings for identical products with differences only in price, shipping

[123] *Intellectual Property Policy*, Temu (Mar. 2, 2025), https://www.temu.com/intellectual-property-policy.html.

[124] Chandra Steele, *What Is Temu? Read Before You 'Shop Like a Billionaire'*, PC Mag (January 15, 2025), https://www.pcmag.com/explainers/what-is-temu-read-before-you-shop-like-a-billionaire.

speed, and other minor details. Temu offers no ability for IP rightsholders to report these identical products except for locating each listing separately and providing Temu with each specific listing URL link to Temu's own listing of the product. IP watchdog groups warn that rightsholders who submit multiple URLs to Temu at once can expect Temu to take significantly longer to provide any response to those complaints than submitting only a single URL in a complaint.[125]

244. As a result of Temu's convoluted and ineffective IP protection policy, the Temu store is rife with unlicensed products listed for sale bearing protected trademark images. Countless brands are impersonated on the store, including the Arizona Cardinals, Fender Guitars, Ping Golf Clubs, Taser, the University of Arizona, Arizona State University, and Northern Arizona University. (See Figures 6–12).

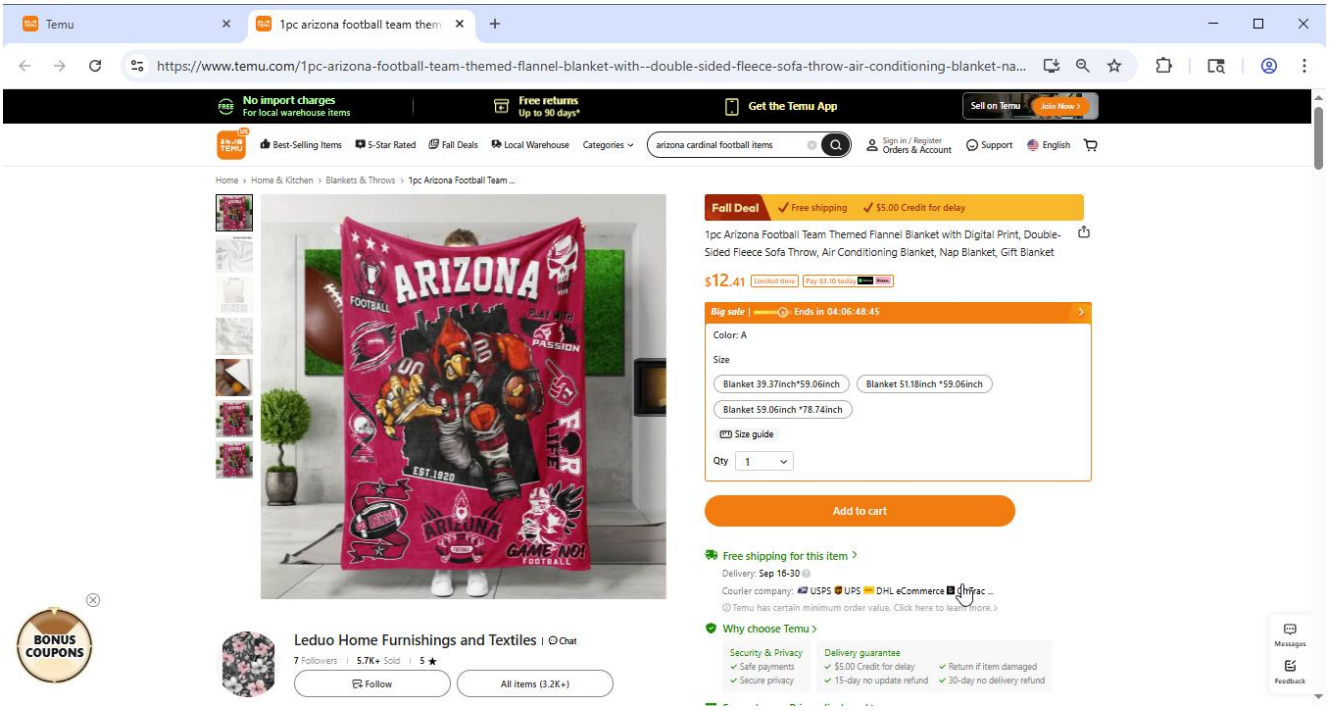

Figure 6: Temu product listing for counterfeit "Arizona Cardinals" merchandise

[125] *Why Removing Counterfeit Listings on Temu Matters*, IP Moat, https://ipmoat.ai/blogs/how-to-guides/how-to-remove-copied-product-listings-from-temu (last visited June 6, 2025).

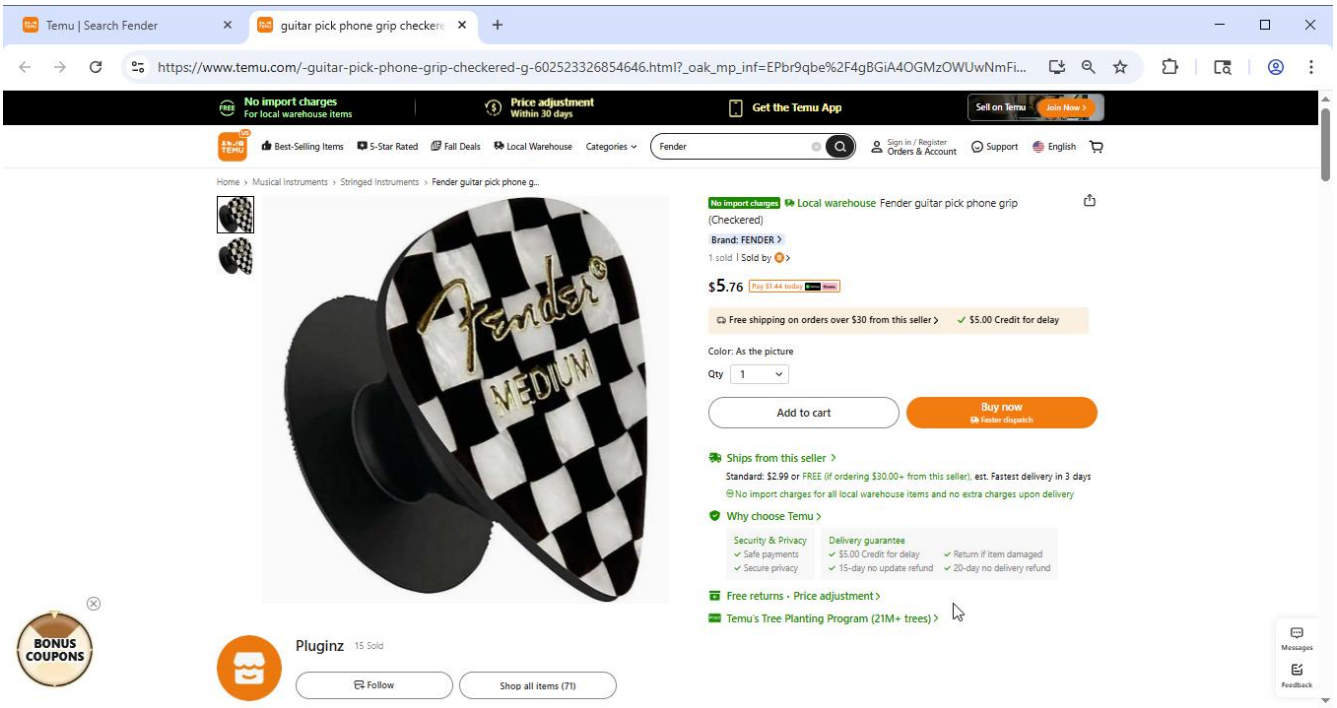

Figure 7: Temu product listings for counterfeit "Fender" merchandise

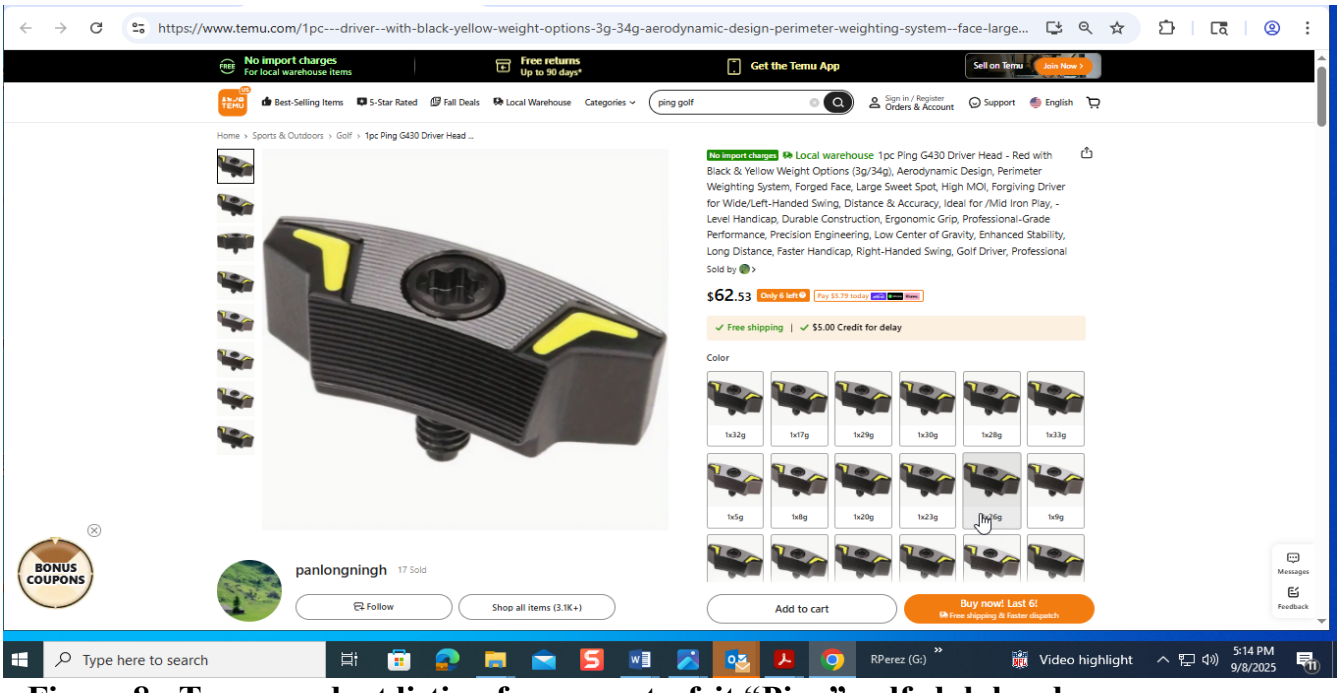

Figure 8: Temu product listing for a counterfeit "Ping" golf club head.

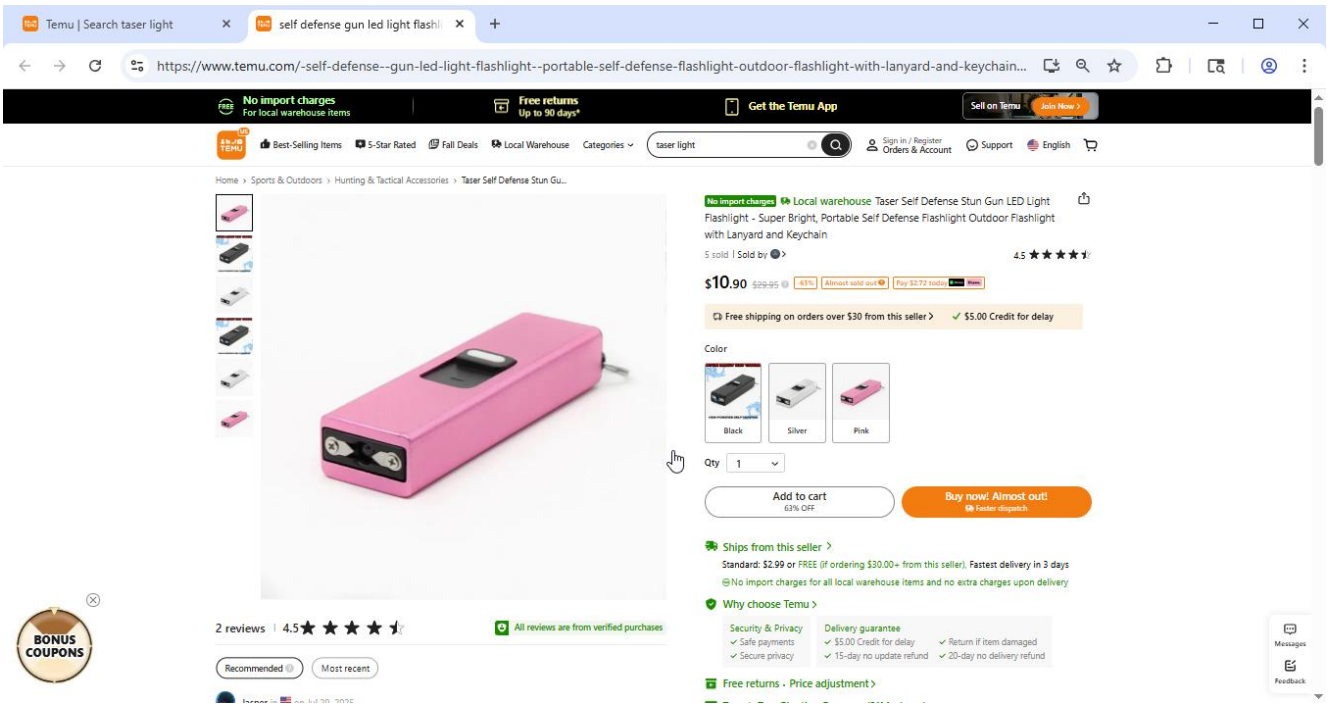

Figure 9: Temu product listing for a counterfeit "Taser" device.

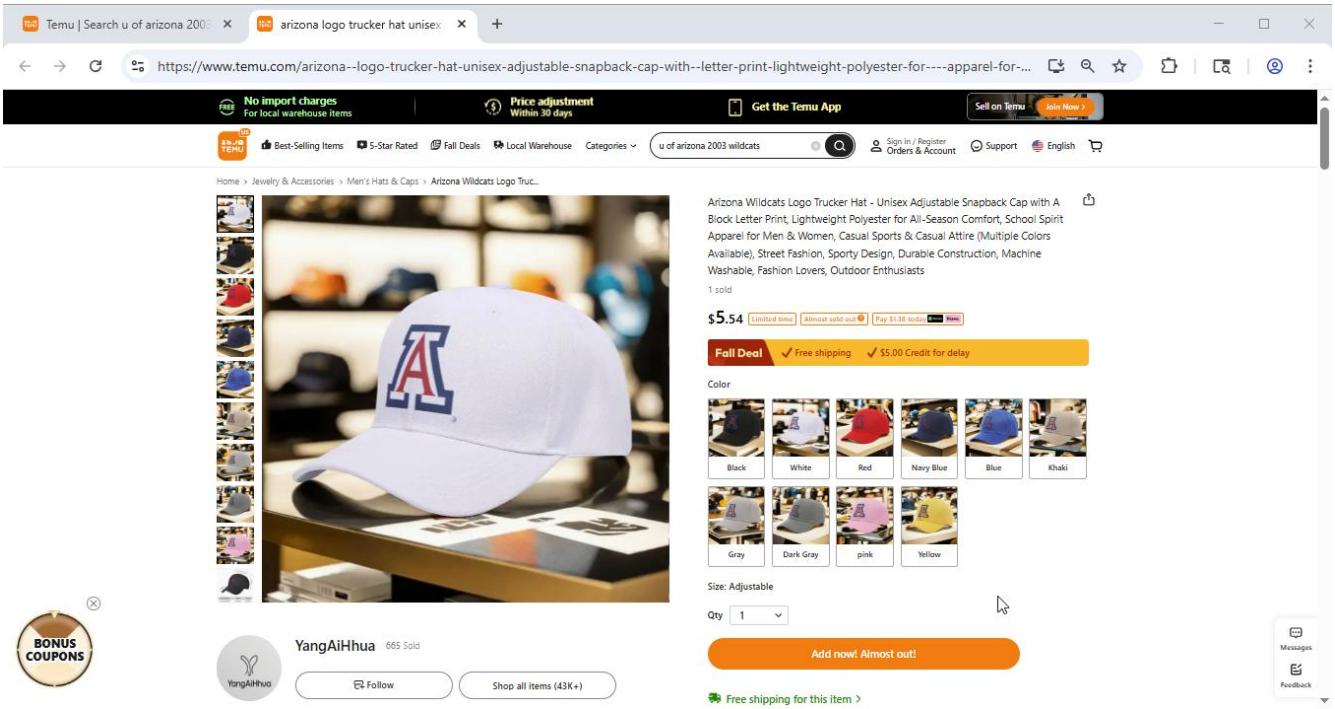

Figure 10: Temu product listing for a counterfeit "University of Arizona" merchandise.

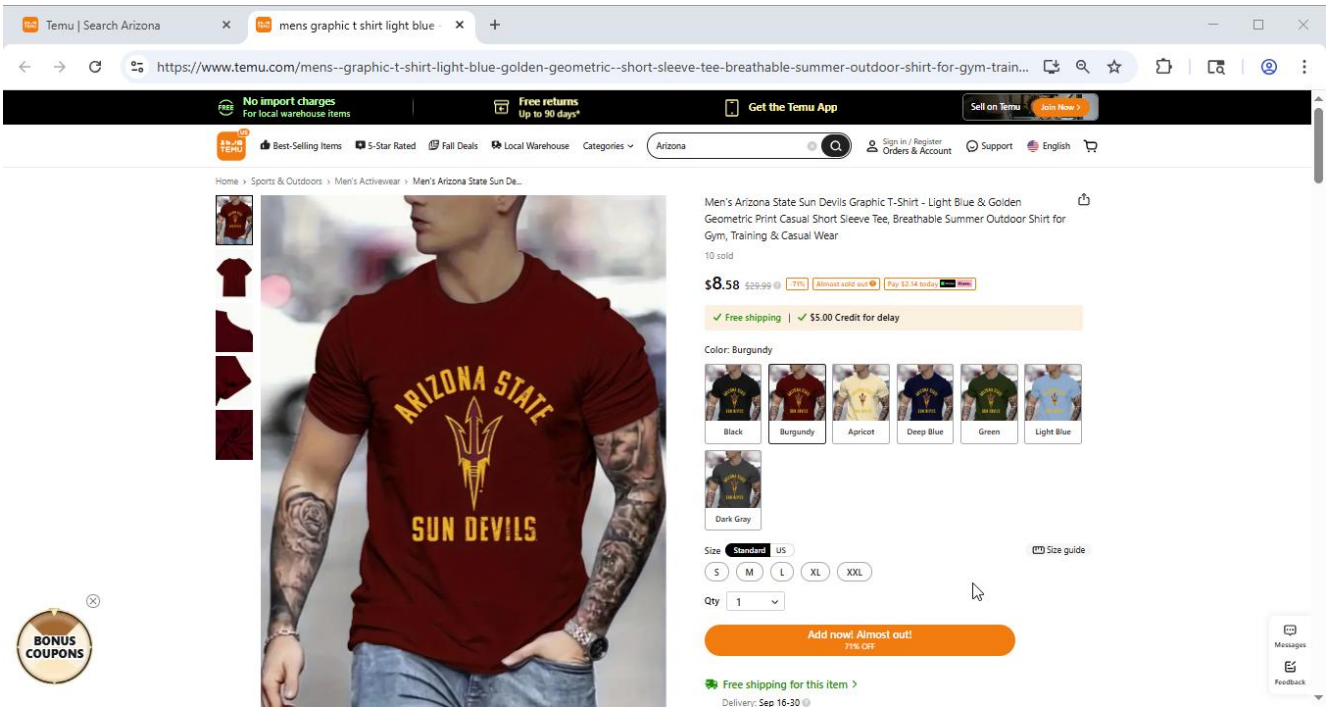

Figure 11: Temu product listing for a counterfeit "Arizona State University" t-shirt.

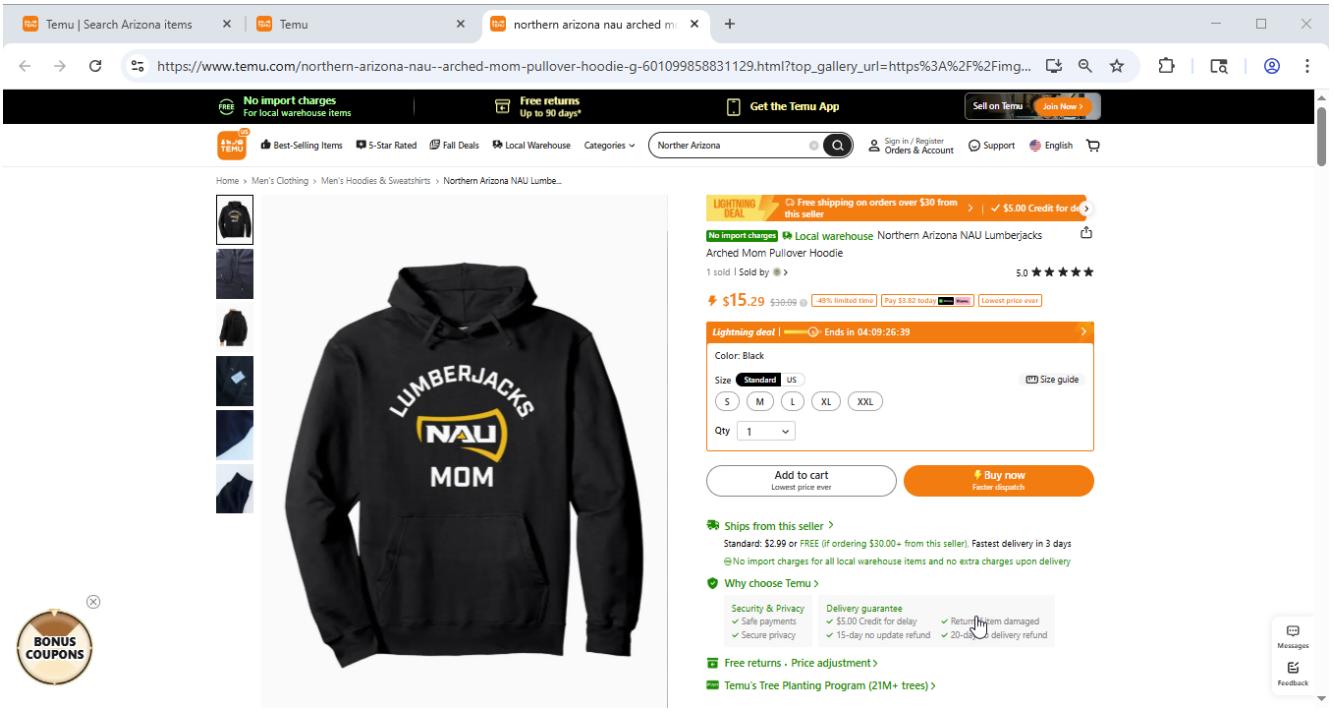

Figure 12: Temu product listing for a counterfeit "Northern Arizona University Lumberjacks" hoodie.

245. These unlicensed products, as well as countless more, are falsely presented to consumers as authentic and licensed by the true owners of those brands.

ix. Deceptive and Unfair Dispute Resolution Process

246. Beyond the surreptitious collection of Arizonans' PII, and the unlawful and deceptive trade practices described herein, Defendants further violate the laws of Arizona by engaging in bad faith in the course of dispute resolution with their customers.

247. Specifically, Defendants' terms of service for Temu purports to require that all disputes between consumers and Temu be resolved through binding arbitration—meaning that consumers are required to surrender their Seventh Amendment right to a jury trial and must instead submit to an extra-judicial dispute resolution process through a third-party arbitrator that is not subject to judicial review.

248. But even this defense-friendly forum is not enough for Temu. Recently, a complaint was filed in the Eastern District of New York seeking to compel Temu to follow through with arbitrations filed by at least several thousand customers, with whom Temu refused to arbitrate.

249. Specifically, in *McMahan, et al. v. Whaleco Inc.*, 1:25-cv-01590 (E.D.N.Y.), the plaintiffs stated that prior to filing an arbitration, a customer must conduct a settlement conference "in good faith to attempt to resolve the parties' disputes." *See,* 1:25-cv-01590 (ECF No. 1 at ¶ 32).

250. However, should any consumer seek to engage in such a pre-arbitration conference, Temu simply uses that overture as a means of gathering information and then scaring customers "with threats of sanctions should they proceed with their claims." *Id.* at ¶ 37. Attorneys for the *McMahan* plaintiffs said the Temu representatives in question refused to have discussions, and that rather than attempting to resolve the complaints, their purpose was to browbeat and scare consumers into declining to pursue any claims against the company. *See, generally*, *id*.

251. Thus, beyond depriving consumers of the protections of the judicial system, Temu further refuses to allow customers access to *Defendants' own chosen forum for dispute*

resolution. The fact that multiple thousands of Temu customers are unable to resolve their individual claims against Temu, *in any forum*, due to Temu's bullying and obfuscating tactics, is inherently violative of the ACFA.

x. "Greenwashing"

252. In order to further incentivize consumers to purchase products on its site, Temu also deceptively represents that it donates a portion of sales through the app to charity as part of a "Tree Planting Program," by placing information about that program immediately below the "Add to cart" button, "Free shipping" information, and "Free returns" information on the product page.

253. Temu claims that it has planted over 19 million trees, through a charity called "Trees for the Future," without disclosing any information about what portion of each sale is donated to charity. Temu claims that donations to Trees for the Future are "funded by users worldwide who donate by clicking 'Donate with Temu' at checkout *and by Temu*."[126] (Emphasis added). Trees for the Future displays its "Corporate Partners" on its website, ranking them by the "number of trees planted" by each partner. The charity lists eleven "Corporate Partners" that have "planted" more than 1-million trees. Temu is listed as the third largest "tree planter," with "18-million trees planted." According to Trees for the Future's 2023 audited financial statements, the charity received over $12.8 million in total contributions and grants in 2023.[127]

254. On information and belief, Temu's annual revenue in 2023 was approximately $18-billion. Even assuming that the donations to Trees for the Future are funded entirely by Temu from its business revenue, and none of the donations were funded by individual Temu customers making the donations *in addition* to payment for purchases from Temu, the most generous possible calculation of Temu's own contributions to Trees for the Future would account for less than one third of one tenth of one percent (.03%) of Temu's total revenue in 2023. This ratio is not disclosed to customers when they make a purchase from Temu.

---

[126] *Temu's Tree Planting Program*, Temu, https://www.temu.com/tree-landing.html (last visited June 6, 2025).

[127] *Financial Statements for the Year Ended December 31, 2023*, Trees for the Future 5 (Nov. 15, 2024), https://trees.org/wp-content/uploads/2024/11/TREES-2023-Audit-Report.pdf.

V. CLAIMS FOR RELIEF

COUNT I

VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT

A.R.S. §§ 44-1521 to -1534

(Deceptive Acts and Practices)

255. The State re-alleges and incorporates by reference all prior allegations of this Complaint as though fully set forth herein.

256. The conduct described in the preceding paragraphs of this Complaint constitutes deception, deceptive or unfair acts or practices, fraud, false pretenses, false promises, misrepresentations, or concealment, suppression or omission of material facts with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of merchandise in violation of the ACFA, A.R.S. §§ 44-1521 to 44-1534.

257. Defendants are "persons" within the meaning of A.R.S. § 44-1521(6).

258. Defendants are engaged in the sale and advertisement of tangible merchandise to Arizonans through the Temu app, as defined in A.R.S. § 44-1521(5).

259. The Temu app is itself an intangible product and service under A.R.S. § 44-1521(5).

260. Defendants engaged in deceptive acts and practices to surreptitiously collect Arizona consumers' sensitive PII without their knowledge.

261. As more fully described in Sections IV(A) through (I) above, from September 2022 through the present, Defendants have engaged in deceptive acts and practices to mask the Temu app's behavior, hide the fact that PII is being siphoned from the user's device, and prevent the user from knowing that said PII is subject to unfettered use by other individuals and a foreign government with its own agenda. These deceptive acts and practices include, but are not limited to:

a. failing to inform users in its privacy policies or elsewhere that the Temu app collects and catalogues information about all WiFi networks that can be detected

///

by the user's device, whether or not the device is actually connected to those WiFi networks;

b. failing to inform users in its privacy policies or elsewhere that the Temu app obtains access to the user's microphone and can record audio from that microphone;

c. misrepresenting to users in its privacy policies and elsewhere either that the Temu app collects only the user's general location data, or that the Temu app does not collect any location data when in reality the app collects precise, granular location data;

d. failing to inform users in its privacy policies and elsewhere that the Temu app collects and catalogues private information about the user's phone calls made from the device and connections to mobile service providers; and

e. failing to inform users in its privacy policies and elsewhere that the Temu app collects lists of other apps installed on the user's device and the user's activities on those apps.

262. As more fully described in Section IV(J) above, from September 2022 through the present, Defendants have engaged in deceptive acts and practices in the offer and sale of products on the Temu app and during the course of their resolutions of consumer complaints. These deceptive acts and practices include, but are not limited to:

a. misrepresenting the quality, features, functionality, and other important characteristics of products offered for sale on the Temu app;

b. misrepresenting the ordinary price of goods for sale on the Temu app and representing to consumers that products are offered at steep discounts for limited time periods when the price of the products are not actually discounted or time limited;

c. misrepresenting that products offered for sale on the Temu app are authentic and licensed by copyright and trademark holders when those products are not authentic, licensed, or approved by the copyright and trademark holders;

d. falsely representing to consumers that Temu would donate a substantial portion of their purchase price to an environmental charity; and

e. manipulating product reviews posted by legitimate purchasers and posting fictional product reviews to misrepresent the quality of the goods and services the purchasers received from Temu to future consumers.

263. Each and every instance of unfair, false, misleading, and/or deceptive conduct constitutes a separate and independent violation of the ACFA.

264. While engaging in the acts and practices alleged in this Complaint, Defendants knew or should have known that their conduct was of the nature prohibited by A.R.S. § 44-1522, subjecting themselves to enforcement and penalties as provided in A.R.S. § 44-1531(A).

COUNT II

VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT

A.R.S. §§ 44-1521 to -1534

(Omission/Deceptive Practices)

265. The State realleges and incorporates by reference all prior allegations of this Complaint as thought fully set forth herein.

266. Concealment, suppression, or omission of material facts with intent that others rely on such concealment, suppression, or omission, in connection with the sale or advertisement of merchandise is a violation of the ACFA, A.R.S. §§ 44-1521 to 44-1534.

267. Pursuant to Arizona law, a practice of omitting information in connection with the sale and advertisement of merchandise may be a deceptive practice in violation of the ACFA. *State ex rel. Horne v. AutoZone, Inc.*, 229 Ariz. 358, 361 (2012).

268. As more fully described in Sections IV(A) through (I) above, from September 2022 through the present, Defendants have utilized deception—in the forms of omission and deliberate concealment—to mask the Temu app's behavior, hide the fact that PII is being siphoned from the user's device, and prevent the user from knowing that said PII is subject to unfettered use by other individuals and a foreign government with its own agenda. These omissions and concealments include, but are not limited to:

a. failing to inform users in its privacy policies or elsewhere that the Temu app collects and catalogues information about all WiFi networks that can be detected by the user's device, whether or not the device is actually connected to those WiFi networks;

b. failing to inform users in its privacy policies or elsewhere that the Temu app obtains access to the user's microphone and can record audio from that microphone;

c. misrepresenting to users in its privacy policies and elsewhere either that the Temu app collects only the user's general location data, or that the Temu app does not collect any location data when in reality the app collects precise, granular location data;

d. failing to inform users in its privacy policies and elsewhere that the Temu app collects and catalogues private information about the user's phone calls made from the device and connections to mobile service providers;

e. failing to inform users in its privacy policies and elsewhere that the Temu app collects lists of other apps installed on the user's device and the user's activities on those apps.

269. As more fully described in Section IV(J) above, from September 2022 through the present, Defendants have utilized deception—in the form of omission and deliberate concealment—in the offer and sale of products on the Temu app and during the course of their resolutions of consumer complaints. These omissions and concealments include, but are not limited to:

a. failing to inform consumers that products offered for sale on the Temu app lack important features, functionality, or other important characteristics that a reasonable consumer would expect the products to have;

b. failing to inform consumers that the products offered for sale on the Temu app are manufactured through the use of forced labor;

///

c. failing to inform consumers about the full terms and conditions of promotional offers on the Temu app; and

d. failing to inform consumers that products offered for sale on the Temu app are unlicensed or unauthorized reproductions of products licensed and approved by intellectual property holders.

270. These omissions were consistent, pervasive, and had the tendency and capacity to mislead consumers, and their uses were, therefore, deceptive practices in violation of A.R.S. § 44-1522.

271. These omissions were material to user's decisions to use the Temu app and purchase products from Temu, and Defendants intended Temu users and consumers to rely on those material omissions when interacting with the Temu app service and purchasing goods from Temu.

272. Defendants knew or should have known that their omissions and deceptive practices described herein were of the nature prohibited by A.R.S. § 44-1522, and were therefore willful, subjecting Defendants to civil penalties as provided in A.R.S. § 44-1531.

273. Defendants committed separate and independent violations of the ACFA through each and every unfair, deceptive, false, or misleading representation, or omission of material information.

COUNT III

VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT

A.R.S. §§ 44-1521 to -1534

(Unfair Practices)

274. The State realleges and incorporates by reference all prior allegations of this Complaint as thought fully set forth herein.

275. The ACFA prohibits the use of "unfair" acts and practices in connection with the sale or advertisement of merchandise.

///

///

276. Unfair acts and practices are those that are harmful to consumers, not reasonably avoidable by consumers, and not outweighed by countervailing benefit to consumers or to competition.

277. As more fully described in Sections IV(A) through (I) above, from September 2022 through the present, Defendants' have engaged in unfair acts or practices in order to surreptitiously collect users' PII in a manner that is unknown—and due to the intentional design of the Temu app—potentially unknowable to users. These unfair acts or practices include, but are not limited to:

a. creating an app that purported to be an e-commerce platform which exploits vulnerabilities in smartphone operating systems to obtain access to PII on the device that apps are not meant to have; and

b. including features and functionality in the Temu app that are not necessary or appropriate to carry out the app's purpose as an e-retail platform but instead are included only for the purpose of collecting users' PII.

278. Defendants' conduct is so extreme that the two dominant app marketplaces—Apple and Google—have had to intervene due to the privacy harms (and the misrepresentations, omissions, and concealment in furtherance of those harms) visited upon users, including users in Arizona.

279. The fact that the Temu app's privacy-violative conduct is executed through code—in a manner that is invisible to the layperson—makes the conduct complained of all the more egregious, as there is no way for Arizonans to know the full extent of the nature of the privacy harms visited upon them by the app.

280. Defendants' conduct is especially egregious in light of the lengths to which they go to prevent independent third parties—including security researchers, Google, and Apple—from uncovering their bad acts.

281. As more fully described in Section IV(J) above, from September 2022 through the present, Defendants have engaged in unfair practices in the offer and sale of products on the

///

Temu app and during the course of their resolutions of consumer complaints. These unfair practices include, but are not limited to:

a. refusing to honor and abide by the terms of Temu's own return policy;

b. charging consumers for goods that were not delivered to the consumer;

c. charging consumers for goods they did not order from Temu;

d. engaging in the use of pyramid and chain letter-like marketing schemes to induce users to sign up for their platform and providing Temu with PII for the users' friends and contacts;

e. using PII acquired from users about their friends and contacts to send large volumes of unsolicited emails, text messages, and other unwanted contacts to those friends and contacts;

f. changing the terms of promotional offers to require further actions from consumers to obtain the promised rewards after consumers complete the initially stated requirements;

g. failing to honor the stated terms of promotional offers presented to Temu app users even after the users complete all of the stated requirements to receive the promotional reward;

h. requiring consumers to accept refunds of the price paid for goods the consumer return to Temu in the form of store credit;

i. restricting consumers' use of store credit from returned goods such that consumers are required to spend more money with Temu than the value of the store credit in order to use the store credit toward the cost of future purchases;

j. placing unfair requirements on consumers desiring to engage in formal dispute resolution with Temu by requiring consumers to first undergo an oppressive process of pre-arbitration meetings at which consumers must listen to a Temu representative intimidate and threaten the consumers if they persist in their formal dispute process.

///

282. Defendants' unfair acts and practices identified in ¶¶ 277 and 281 were harmful to Arizona consumers.

283. The harm caused by Defendants' acts and practices was not reasonably avoidable by consumers.

284. Defendants' acts and practices were not outweighed by any benefit to consumers or competition.

285. At all times, Defendants' knew or should have known that their conduct was unfair, and their conduct was willful pursuant to A.R.S. § 44-1531.

PRAYER FOR RELIEF

Wherefore, the State respectfully requests that the Court:

286. Pursuant to A.R.S. § 44-1528(A)(1), issue a permanent injunction in accordance with Ariz. R. Civ. P. 65(d)(1), enjoining and restraining (a) Defendants, (b)their officers, agents, servants, employees, attorneys, and (c) all persons in active concert or participation with anyone described in part (a) or (b) of this paragraph, directly or indirectly, from engaging in deceptive, misleading, or unfair acts or practices, or concealments, suppressions, or omissions, that violate the ACFA, A.R.S. § 44-1522(A), including specific injunctive relief barring Defendants from engaging in the unlawful acts and practices set forth above;

287. Pursuant to A.R.S. § 44-1528(A)(2), order Defendants to restore to all persons in interest any monies or property, real or personal, which may have been acquired by any means or any practice in this article declared to be unlawful;

288. Pursuant to A.R.S. § 44-1528(A)(3), order Defendants to disgorge all profits, gains, gross receipts, or other benefits obtained as a result of their unlawful acts alleged herein;

289. Pursuant to A.R.S. § 44-1531, order Defendants to pay to the State of Arizona a civil penalty of up to $10,000 for each willful violation by each Defendant of A.R.S. § 44-1522;

290. Pursuant to A.R.S. § 44-1534, order Defendants to reimburse the State for its costs and attorneys' fees incurred in the investigation and prosecution of Defendants' activities alleged in this Complaint;

///

291. Pursuant to A.R.S. § 44-1201, require Defendants to pay pre-judgment and post-judgment interest to the State and all consumers;

292. Award the State such further relief the Court deems just and proper under the circumstances.

DATED this 1st day of December, 2025.

KRISTIN K. MAYES
Attorney General

By: Alyse Meislik

Alyse C. Meislik (024052)
Assistant Attorney General
OFFICE OF THE ATTORNEY GENERAL
2005 North Central Avenue
Phoenix, Arizona 85004-1592
Tel: (602) 542-3725
Alyse.Meislik@azag.gov
consumer@azag.gov

N. Majed Nachawati II
Brian E. McMath, *Pro Hac Vice pending*
Brian L. Moore, *Pro Hac Vice pending*
NACHAWATI LAW GROUP
5489 Blair Road
Dallas, Texas 75231
Telephone: (214) 890-0711
bmcmath@ntrial.com
bmoore@ntrial.com

David F. Slade, *Pro Hac Vice pending*
WADE KILPELA SLADE
1 Riverfront Place, Suite 745
North Little Rock, Arkansas 72114
slade@waykayslay.com
Attorneys for the State of Arizona