<div align="center">

COMMONWEALTH OF KENTUCKY
WOODFORD CIRCUIT COURT, DIV. _____
CIVIL ACTION NO. _____

</div>

COMMONWEALTH OF KENTUCY, *ex rel.*
RUSSELL COLEMAN, ATTORNEY GENERAL,

Plaintiff,

v.

PDD HOLDINGS, INC. F/K/A
PINDUODUO INC.; and WHALECO,
INC. D/B/A/ TEMU;

Defendants.

<div align="center">

COMPLAINT

JURY TRIAL DEMANDED

</div>

The Plaintiff, the Commonwealth of Kentucky ("Kentucky" or "the Commonwealth"), 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 Kentucky Consumer Protection Act, KRS 367.110, *et seq*. ("KCPA") as well as Kentucky common law. In support of its claims, the Commonwealth states as follows:

I.   INTRODUCTION

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

2.   The harms committed against Kentucky 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 (¶¶ 45-198) involves threats to Kentuckians' 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 KCPA, this additional geopolitical component amplifies the consequences of that existing violation.

4.   The second harm, discussed in Section IV.J of the Complaint (¶¶ 199-236), involves more traditional consumer deception. Temu sells products to Kentuckians in ways that are plainly violative of the KCPA, 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.
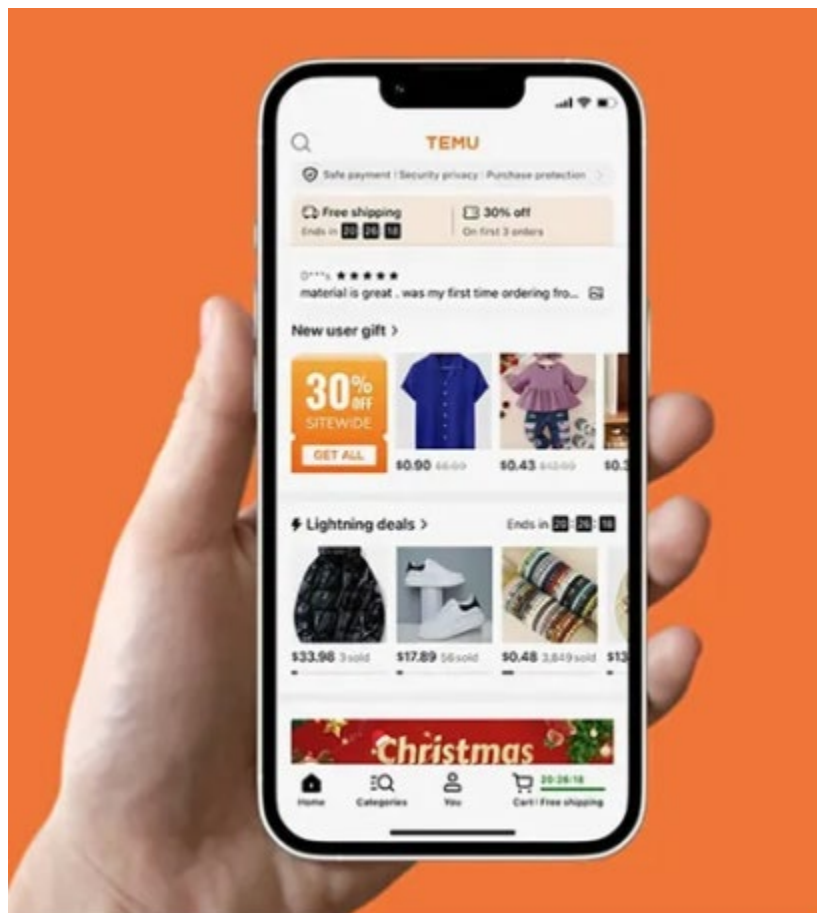
Figure 1: Representation of the Temu mobile application.

3

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 the Commonwealth of Kentucky, with usage driven both via word of mouth and by an aggressive, multibillion dollar marketing campaign. This campaign recently made headlines for three separate

4

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

---

[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] 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/.

[6] 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.

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 overlay.

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 so that it can 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 (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 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 phone.

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 even goes 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 Kentucky 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 Kentucky 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 Kentucky brands like the University of Kentucky, University of Louisville, Buffalo Trace Distillery and Churchill Downs.

24.　　Accordingly, the Commonwealth brings this action pursuant to the KCPA and Kentucky's common law and seeks a preliminary and permanent injunction preventing Defendants from acquiring, maintaining, and otherwise utilizing the PII of Kentucky citizens, preventing Defendants from allowing widespread intellectual property infringement to the detriment and

---

[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/.

confusion of Kentucky consumers, and further seeks civil penalties in light of Defendants' conduct, as well as all other available relief allowed by law.

II.   JURISDICTION AND VENUE

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

26.   Woodford Circuit Court has subject matter jurisdiction over the claims submitted pursuant to KRS 23A.010, KRS 315.235, and KRS 367.190 as the claims enumerated herein arise exclusively under Kentucky statutory and common law and from the *parens patriae* authority of the Attorney General to act on behalf of the Commonwealth and its citizens. The Commonwealth's

claims are in excess of any minimum dollar amount necessary to establish the jurisdiction of the

Court.

27.   Kentucky 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 Commonwealth is not a citizen of any state.

28.   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 Commonwealth 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).

29.   Specifically, the causes of action asserted, and the remedies sought herein, are

founded upon the positive statutory, common, and decisional laws of Kentucky. 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.

30.   In this Complaint, to the extent Kentucky cites or alludes to federal statutes,

regulations, or agency memoranda, it does so only to establish Defendants' knowledge, to state the

duties owed under Kentucky 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.

31.   Venue is appropriate in Woodford Circuit Court under KRS 452.460, which allows venue in the county where the injury was suffered. Where the injury is suffered by the Commonwealth, its agents or employees, or the Commonwealth as a whole, venue is proper in Woodford Circuit Court.

III.   PARTIES

A. The Commonwealth of Kentucky

32.   Plaintiff, the Commonwealth of Kentucky, brings this action, by and through its Attorney General, Russell Coleman, in its sovereign capacity to protect the interests of the Commonwealth and its citizens. The Attorney General is authorized to take action against Defendants for violation of state laws and regulations. Russell Coleman is the duly elected Attorney General of Kentucky, an independent constitutional officer of the Commonwealth and its chief law officer, with full authority to initiate and prosecute all cases in which the Commonwealth has an interest. The Attorney General is vested with specific constitutional, statutory and common law authority to commence proceedings to enforce KRS 218A.240, KRS 315.235, KRS 367.110 *et seq*., to initiate actions necessary to exercise all common law duties and authority pertaining to the office of the Attorney General under the common law pursuant to KRS 15.020, and pursuant to the Attorney General's *parens patriae* authority, to bring an action on behalf of the Commonwealth and its citizens.

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

33.   Defendant PDD Holdings Inc. ("PDD Holdings"), is a company that was founded in China in 2015 under the name Pinduoduo, and which is registered in the Cayman Islands. It owns and operates a portfolio of businesses and is listed on the Nasdaq exchange in 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.

34.   PDD Holdings is 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

35.   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

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

37.   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 the Defendant Temu.

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

---

[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.

39.   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]

40.   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 Commonwealth of Kentucky, to facilitate transactions between Kentucky consumers and Chinese merchants in part using data and information gathered about Kentucky consumers unlawfully, as described below.

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

42.   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 Kentucky, discussed *infra* at ¶¶ 108-112.

43.   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.

44.   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

---

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

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.

45.   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]

46.   Among other business activities, PDD Holdings operates Pinduoduo, an e-

commerce app created in China that offers consumer products across a spectrum of categories.

47.   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]

---

[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).

48.   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.

49.   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.

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

50.   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]

---

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

[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.

51.   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]

52.   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]

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

54.   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]

55.   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]

56.   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

---

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

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.

57.　　　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]

58.　　　Moreover, once the app was installed, the app was able to continue running in the

background and prevent itself from being uninstalled.[24]

59.　　　One security researcher interviewed by CNN described Pinduoduo as "the most

dangerous malware ever found among mainstream apps." [25]

60.　　　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.

61.　　　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.

62.　　　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]

---

[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*

17

63.   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]

64.   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 Market in the United States and Kentucky.

65.   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]

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

67.   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]

68.   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, and after-sales services for merchants on its platform. "Temu's network now includes more than 80,000 suppliers."[31]

69.   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

---

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

result, the market capitalization of Defendant PDD Holdings has swelled to over $144 billion as of July 9, 2025.[33]

70.   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 Kentucky—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.

71.   Just like the Pinduoduo app, Temu is using the inducement of low-cost goods to lure users into unknowingly providing near-limitless access to their PII. Such acts are deceptive and unconscionable under Kentucky law.

72.   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.*

73.   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 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

---

[33] Yahoo!Finance, https://finance.yahoo.com/quote/PDD/ (last visited June 2, 2025, 4:20 PM).

   1.   [34] Staff of H.R. Select Comm. on the CCP, *supra* note 31, at 8.

be tracked on the internet [which is an option that all apps in Apple's online marketplace are required to provide to users]."[35]

74.   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]

75.   The Commonwealth'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.

76.   These concerns are addressed more fully as follows:

i. Design and Programming That Intentionally Evades Scrutiny

1. <u>Dynamic recompilation using the "Manwe" tool</u>

---

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

77.   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.

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

79.   Instead, this code enables the app to change its behavior—including its functionality—*on the user's phone*, without anyone being able to know, much less prevent such a change.

80.   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.

81.   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.

82.   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.

83.   And, as noted below, Temu also borrowed code from Pinduoduo in the form of the ZipPatch library (*see* ¶ 111, *infra*), which also allows the app to update its code without pushing the update through Google or Apple.

2. <u>Omission of data collection practices from the Temu app manifest file</u>

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

85.   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 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 SMS, or certain system features, such as the camera and internet access. Each permission is identified by a unique label."[39]

86.   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.

87.   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.

88.   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* ¶¶ 114-119, *infra*.

89.   What this means is that Temu was creating the impression that it did not want nor use its customers' location data, but in reality was getting the information from sources that it could avoid disclosing in the permission manifest.

90.   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

---

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

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

91.   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 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

92.   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.

93.   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.

94.   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.

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

5. Searching for "debuggers"

96.   Much 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]

97.   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

98.   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]

---

[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).

[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).

24

99.   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.

100.   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

101.   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."

102.   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, 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.

103.   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.

104.   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.

25

105.   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.

106.   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.

107.   The Commonwealth'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 Commonwealth'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

108.   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

109.   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.   Further, specific code overlap

110.   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.

111.   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.

27

3. SDK overlap

112. SDKs—otherwise known as Software Development Kits—are distinct libraries of code meant to perform specific functions. Some SDKs handle identifying and compiling statistics about app performance, others serve targeted ads, others render graphics in an app, etc. Temu and Pinduoduo have always had an overlap of multiple SDKs, with an overlap of 34 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

113. 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

114. 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, the permission, ACCESS_FINE_LOCATION, historically was removed from the Temu app's Android manifest for a period of time in 2023, only to reappear once Temu had been called out for this conduct, demonstrating an intent to keep this functionality hidden from the public.

115. Regardless of whether Temu was or was not listing ACCESS_FINE_LOCATION (or ACCESS_COARSE_LOCATION, for that matter) at any point in its history, it was simultaneously acquiring data points from users that allowed Temu to determine users' location even without these permissions. Put another way—Temu was collecting data that would enable it to bypass the location permissions in Android, and simply get its information in a different, more concealed, way.

116.   Many of these data points are discussed below in paragraphs 117 through 119 and 136 through 140.

2.   WiFi access points

117.   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.

118.   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.

119.   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

120.   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

---

[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.

and storage functions of a user's device. These permissions are not adequately disclosed to users, as described in paragraphs 141 through 147 below.

4. Intentional Android exploit: ActivityManager.getRunningTasks

121.   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]

122.   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.

123.   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

---

[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.

common in certain populations like elderly users), the thief can take advantage of this security

lapse and take whatever they wish from inside.

124.   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* ¶¶ 94-97, *supra*.

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

125.   Android Developer documentation explains that this method "[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]

126.   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.).

127.   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]

---

[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).

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

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

129.   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.

130.   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.

131.   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]

132.   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.

---

[48] As explained in paragraphs 53-54, *supra*, the purpose of this data collection was done by Defendants in order "to spy on users and competitors, allegedly to boost sales."

32

- <u>Financial and Payment Apps</u>: PayPal, Klarna, AfterPay, MobilePay, Toss, Swish, and Satispay.

- <u>Miscellaneous</u>: Google Play Store, Google Maps, and the Samsung Galaxy Store.

7. <u>List of all of the accounts a user has stored on the phone</u>

133. 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]

134. 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]

135. 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. <u>Additional sensitive PII</u>

136. 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. Some of the items of PII that Temu collects include:

137. **International Mobile Subscriber Identity ("IMSI")**: these are uniquely-identifying data points that are associated with each mobile phone's unique SIM card. They also

---

[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).

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.

138.   **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 your 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 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.

139.   **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]

140.   **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

---

[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/.

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.

141.   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.

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

143.   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.

144.   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*.

145.   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.

---

[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.

October 17, 2022[53]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 120)	No mention of seeking microphone access (or of audio, generally)
Camera Access (¶ 120)	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."
Location Data (¶¶ 87-90, 114-119, 136-140)	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 (¶¶ 117-119)	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 (¶¶ 121-124; 128-135)	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

---

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

	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 (¶¶ 125-127)	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 (¶¶ 128-135)	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 (¶¶ 136-140)	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 (¶ 120)	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 (¶ 120)	Temu states that it only acquires photos provided by the user, in the course of using the Temu platform: "Personal Information We Collect

---

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

	… 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."
Location Data (¶¶ 87-90, 114-119, 136-140)	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 (¶¶ 117-119)	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 (¶¶ 121-124; 128-135)	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 (¶¶ 125-127)	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 (¶¶ 128-135)	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 (¶¶ 136-140)	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)[.]"

146.   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.

147.   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 (¶ 120)	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 (¶ 120)	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 (¶¶ 87-90, 114-119, 136-140)	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 (¶¶ 117-119)	Temu removed its prior language quoted above and has not provided substitute language.
User's Activity on His or Her Device, Outside of Temu (¶¶ 121-124; 128-135)	Temu removed its prior language quoted above and now states: "Information collected automatically 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:

---

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

	… 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 (¶¶ 125-127)	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 (¶¶ 128-135)	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 (¶¶ 136-140)	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

148.   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.

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

150.   Kentuckians 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.

151.   "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.").

152.   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. Connecticut*, 381 U.S. 479, 486 (1965).

153.   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. United States*, 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).

154.　　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).

155.　　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*.

156.　　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.

157.   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.

158.   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

159.   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.

---

[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.

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

161.   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.

162.   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.

163.   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

---

[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.

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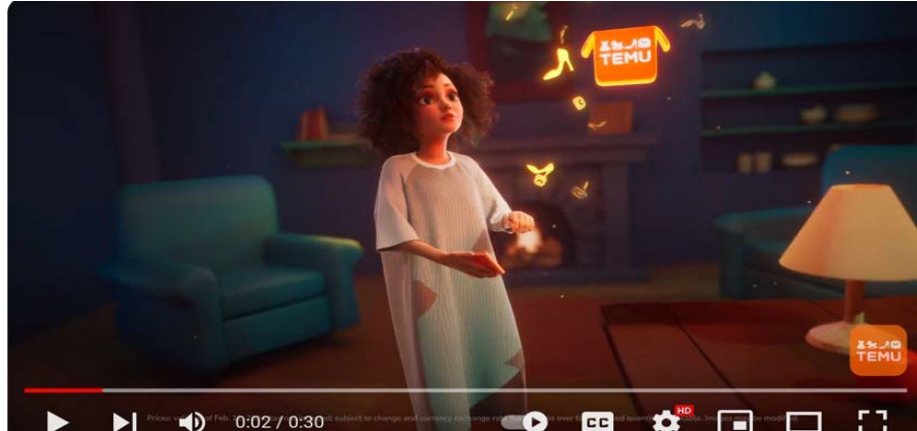
Figure 3: Screen capture of Temu's 2024 Super Bowl commercial.

164.   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.

165.   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

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

of Congress recently sent a letter to Defendants specifically requesting information regarding Temu's data collection practices with respect to minors.[61]

166.   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

167.   While the mere act of invading users' privacy, in the manner described above, is enough to sustain the Commonwealth's claims without any further allegations, there are additional, egregious privacy harms that Kentuckians 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 Kentuckian's data in Defendants' possession—to the government upon request.

168.   Senator Mitch McConnell has expressed concern over China's known "espionage and cyberattacks...to stealing intellectual property and cheating on trade."[62]

169.   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.

170.   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.

---

[61] *See* Letter from Cathy McMorris Rogers & Gus M. Bilirakis to Qin Sun, *supra* note 8, at 3
[62] 167 Cong. Rec. S1580 (2021) (statement of Sen. Mitch McConnell).

171.   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."[63]

172.   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."[64]

173.   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."[65]

---

[63] 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.

[64] 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).

[65] 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/.

174.   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.."[66]

175.   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."[67]

176.   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."[68]

177.   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 use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings . . . ."[69]

178.   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."[70]

---

[66] *Id.* art. 7.
[67] *Id.* art. 14.
[68] *Id.* art. 16.
[69] *Id.* art. 17.
[70] Zheng, *supra* note 63.

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

180.   "China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime."[71]

181.   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."[72]

182.   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."[73]

183.   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."[74]

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

185.   For example, Article 35 provides that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall

---

[71] 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.
[72] *Id.*
[73] 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.
[74] *Id.* art. 49.

undergo a national security review organized by the State cybersecurity and informatization

departments and relevant departments of the State Council."[75]

186.   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.[76]

187.   Since the law's enactment, authorities have issued regulations expanding its

scope.[77]

188.   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.[78]

---

[75] *Id.* art. 35.

[76] *Id.* art. 37.

[77] *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..

[78] *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 77; Gong, *supra* note 77. *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).

189.   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,"[79] 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.[80] 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.[81] CAC eventually imposed a $1.2 billion fine on the company.[82]

190.   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."[83]

191.   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."[84]

192.   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[.]"[85]

---

[79] Jamie P. Horsley, *Behind the Façade of China's Cyber Super-Regulator*, DigiChina (Aug. 8, 2022), https://stanford.io/3FPAOYy.
[80] *Id.*; Li, *supra* note 77..
[81] Horsley, *supra* note 79.
[82] *Id.*
[83] 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.
[84] *Id.* art. 24.
[85] *Id.* art. 31.

193.   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."[86] 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."[87]

194.   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 security services, and that there is no meaningful way to resist these requirements, or any pressure brought to bear by the Party.[88]

195.   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.

---

[86] Haldane, *supra* note 63.

[87] 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.

[88] *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).

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.

196.   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.

197.   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 unconscionable practices.

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

198.   None of the above is speculation or hyperbole. In a filing to the SEC on April 28, 2025,[89] Pinduoduo (1) acknowledges that Temu is one of its platforms,[90] 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."[91]

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."[92]

---

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

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."[93]

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 Laws') impose cybersecurity review obligations on [. . .] network platform operators that hold the data of more than one million users[.]"[94]

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."[95]

---

[93] *Id.* at 52.
[94] *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).
[95] PDD Holdings, Form 20-F Annual Report (2024) at 8.

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

199.   Defendants actively utilize deceptive and unconscionable 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."[96]

200.   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)

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

---

[96] *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/.

201.   These gimmicks have been wildly successful: "PDD's TEMU online marketplace is being reported as among the fastest uptaken apps in history."[97]

202.   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," [98] there have been numerous complaints regarding the quality of goods sold on the site as well as the service provided by Temu.

i.   Deceptive Representations as to the Quality of Goods

203.   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.[99] Users experience undelivered packages and poor customer service. Moreover, even when goods are delivered, they are often of low quality, contrary to Temu's marketing and representations.

204.   For example, one analysis observed that "TEMU products as shipped often do not resemble the photos."[100] 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.[101] In addition, while Defendants claim that

---

[97] *Id.*

2.   [98] *About Temu*, Temu (last visited June 6, 2025), https://www.temu.com/about-temu.html.

[99] 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.
[100] Grizzly Research, *supra* note 96.
[101] 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.

they use "world-class manufacturers" and have "strict policies against counterfeit or unsafe goods,"[102] 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).[103]

ii. False Reference Pricing

205. 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.

206. 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.[104] (See Figure 5)

---

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

[103] 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)

[104] 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/.
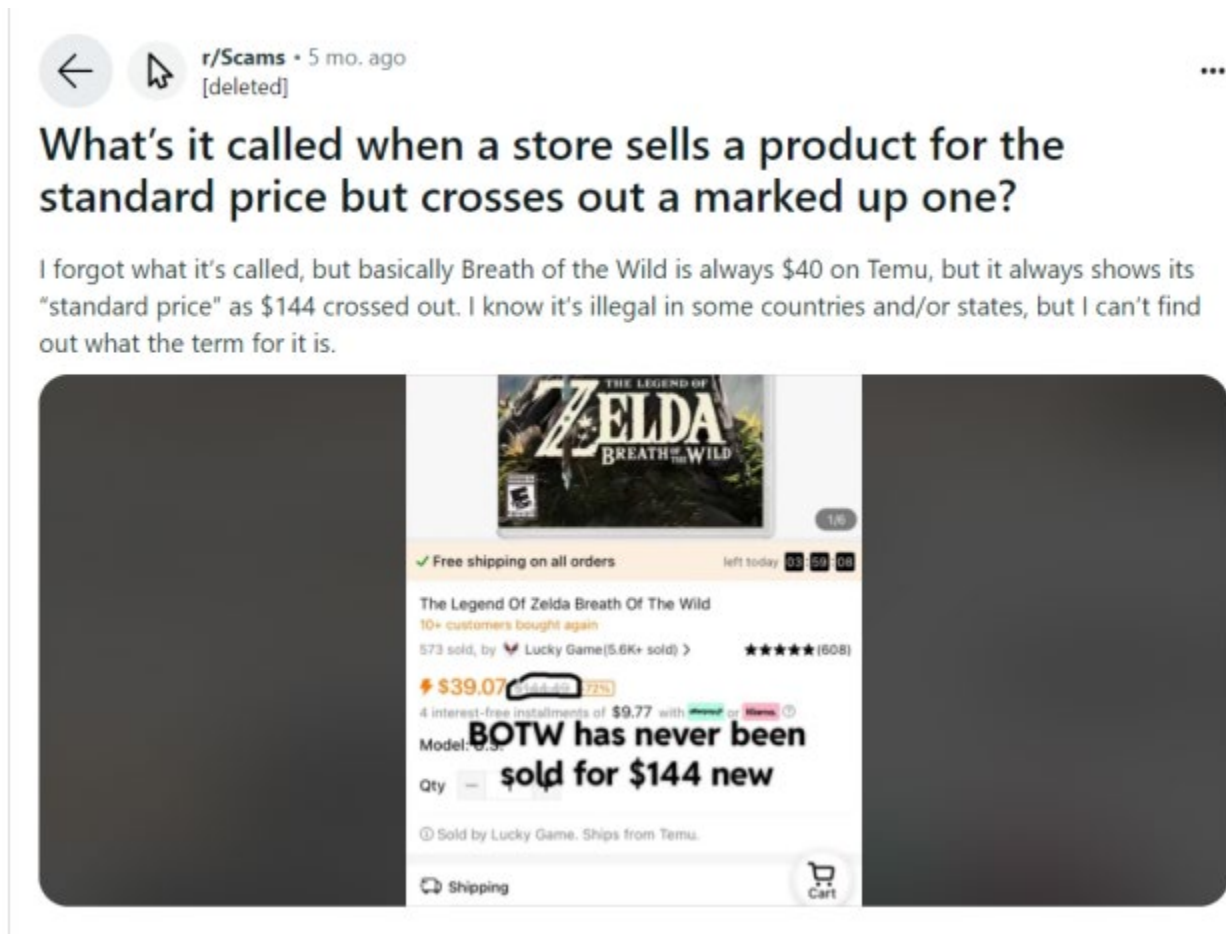
Figure 5: Example of "false reference pricing" on a Temu product listing.

iii. Charges and Delivery for Goods Not Ordered

207.   Numerous Kentucky 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.

208.   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.

209.   One Kentucky consumer made a small purchase from Temu and later discovered that Temu had charged her $833 and shipped an entirely different order to her that she had not ordered.

iv. Use of Forced Labor

210.   In addition, while Defendants claim that they seek to "[d]o good for the world," are "honest, ethical and trustworthy," and are "socially responsible,"[105] 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.[106] 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."[107]

211.   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

---

3.   [105] *About Temu*, Temu (last visited June 6, 2025), https://www.temu.com/about-temu.html.

[106] 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.
[107] *Id.*

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."[108]

212.   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 access"

resulting from such direct-to-consumer sales.[109] 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.[110]

213.   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."[111] 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

---

[108] *Id.*
[109] Kaufman, *supra* note 99.
[110] 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).
[111] Staff of H.R. Select Comm. on the CCP, *supra* note 31, at 2.

on forced labor while relying on tens of thousands of Chinese suppliers to ship goods direct to U.S. consumers."[112] 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.'"[113]

214.   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 CCP's atrocities, which include imprisonment, torture, rape, forced sterilization, and the widespread exploitation of the Uyghur people in forced labor."[114]

215.   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[.]"[115] 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."[116]

216.   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.

---

[112] *Id.*
[113] *Id.*
[114] *Id.* at 3.
[115] *Id.* at 7.
[116] *Id.* at 9.

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

217.   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.

218.   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."[117] "[O]nce you give TEMU your personal 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'."[118] 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.

219.   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."[119]

---

[117] 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/https://www.telegraph.co.uk/business/2023/07/01/temu-china-bargain-basement-amazon-rival-retail-online-shop/.
[118] Grizzly Research, *supra* note 96.
[119] *Id.*

vi. Fake Reviews

220.   Defendants attract and maintain users through other fraudulent means. For example, "TEMU [. . .] compensates users to write reviews," which are then "obviously skewed positive[.]"[120] 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."[121] 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 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."[122] 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.

vii. Gamification

221.   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."[123] 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.

---

[120] *Id.*

[121] *Id.*

[122] 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/.

[123] Titcomb, *supra* note 117.

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

223.   One Kentucky Temu Customer was promised that if they successfully referred if they successfully referred five people to sign up for a Temu account through an affiliate link, Temu would provide the customer with "tickets" to spin a digital wheel to earn money or rewards. When that customer successfully referred five people through their link, Temu did not grant the customer the promised tickets to spin the digital reward wheel.

viii.   Intellectual Property Theft

224.   Temu claims to be "committed to protecting everyone's intellectual property and [to] have a comprehensive policy to that end."[124] 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.[125]

225.   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 speed, and other minor details. Temu offers no ability for IP rightsholders to report these identical products

---

[124] *Intellectual Property Policy*, Temu (Mar. 2, 2025), https://www.temu.com/intellectual-property-policy.html.
[125] 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.

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.[126]

226.   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 Louisville Slugger baseball bats, Maker's Mark Whisky, Jim Beam Kentucky Straight Bourbon Whiskey, Buffalo Trace Kentucky Bourbon Whiskey, the Kentucky Derby at Churchill Downs, Keeneland Race Course, the University of Kentucky, the University of Louisville, Eastern Kentucky University, and Western Kentucky. (See Figures 6–18).
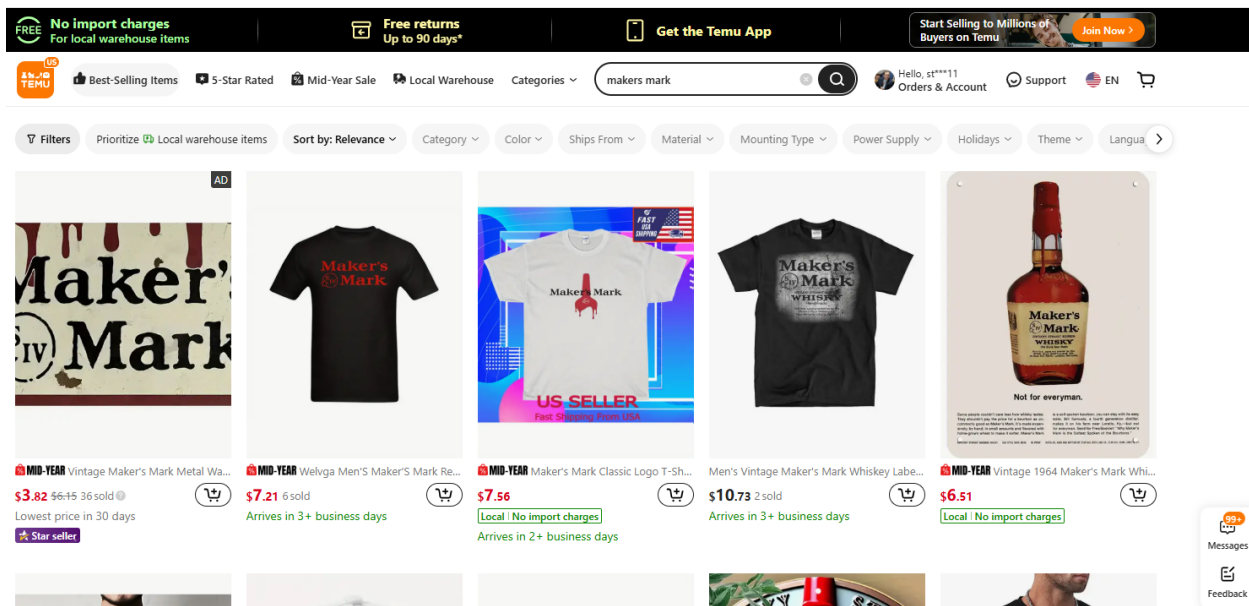

Figure 6: Temu product listings for counterfeit "Maker's Mark" merchandise

---

[126] *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).
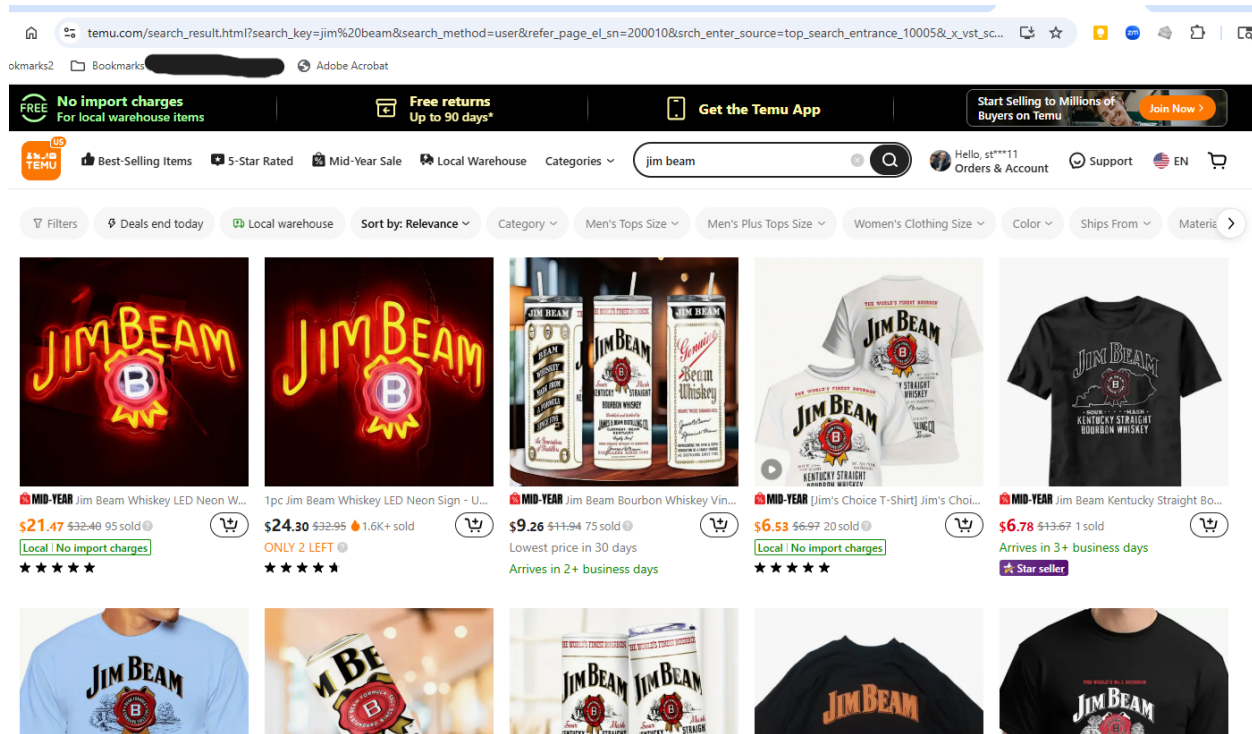
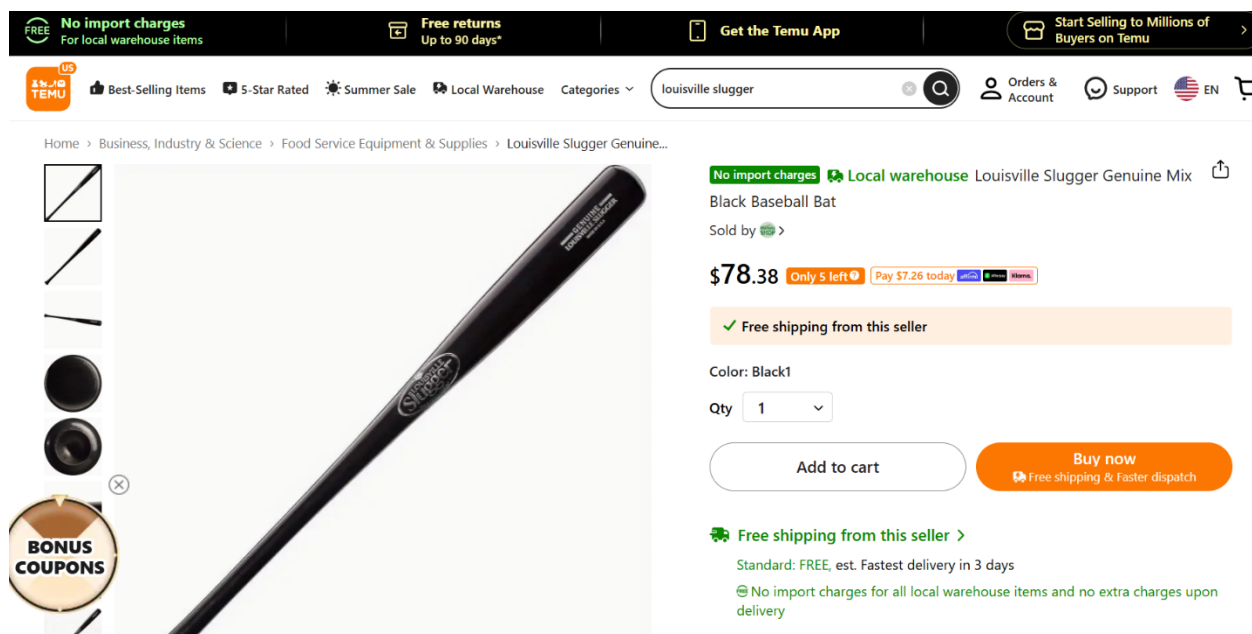**Figure 7: Temu product listings for counterfeit "Jim Beam" merchandise**

Figure 8: Temu product listing for a counterfeit "Louisville Slugger" baseball bat.

67

Product details   Save | Report this item

Material: Polyethylene terephthalate

Item ID: RG2809506 (Copy)

Origin: Guangdong,China

Store Information >

Louisville Slugger Genuine MIX Black Baseball Bat - 33 inches, Cupped, Series 3X Wood, Clear finish, Mixed turning Model

Figure 9: Close up image of counterfeit "Genuine Louisville Slugger" baseball bat with store and origin information.
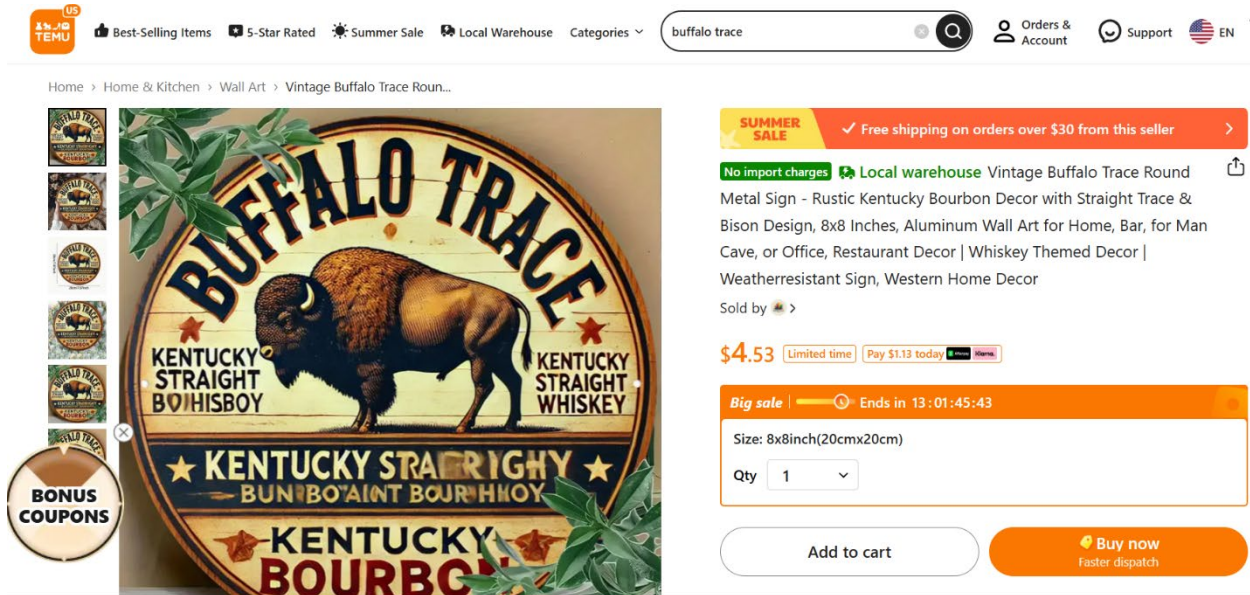
68

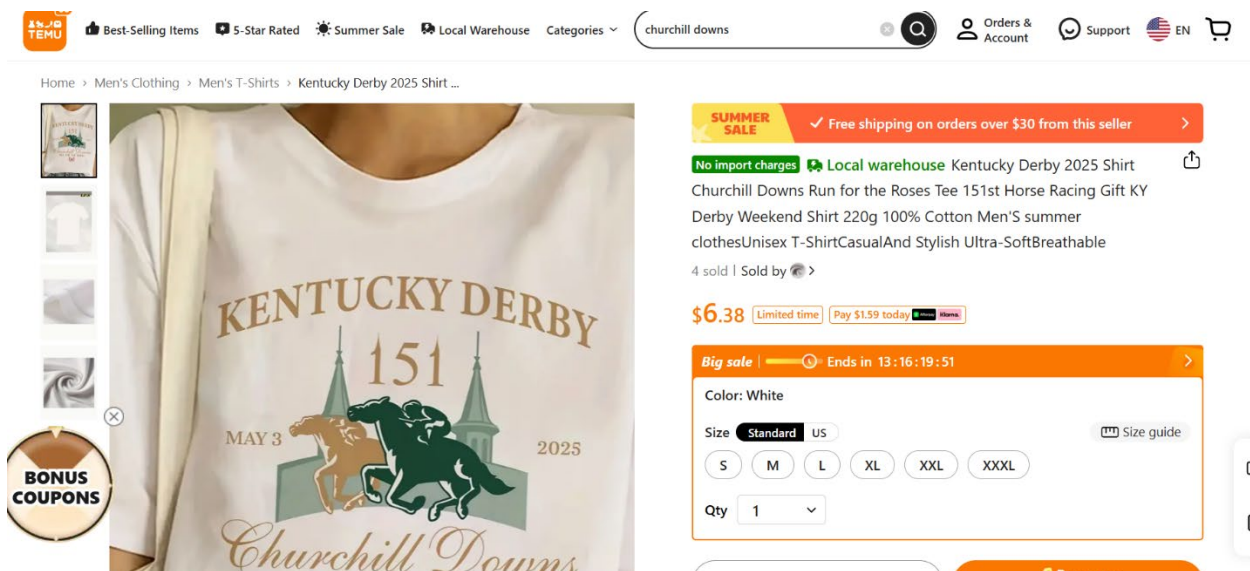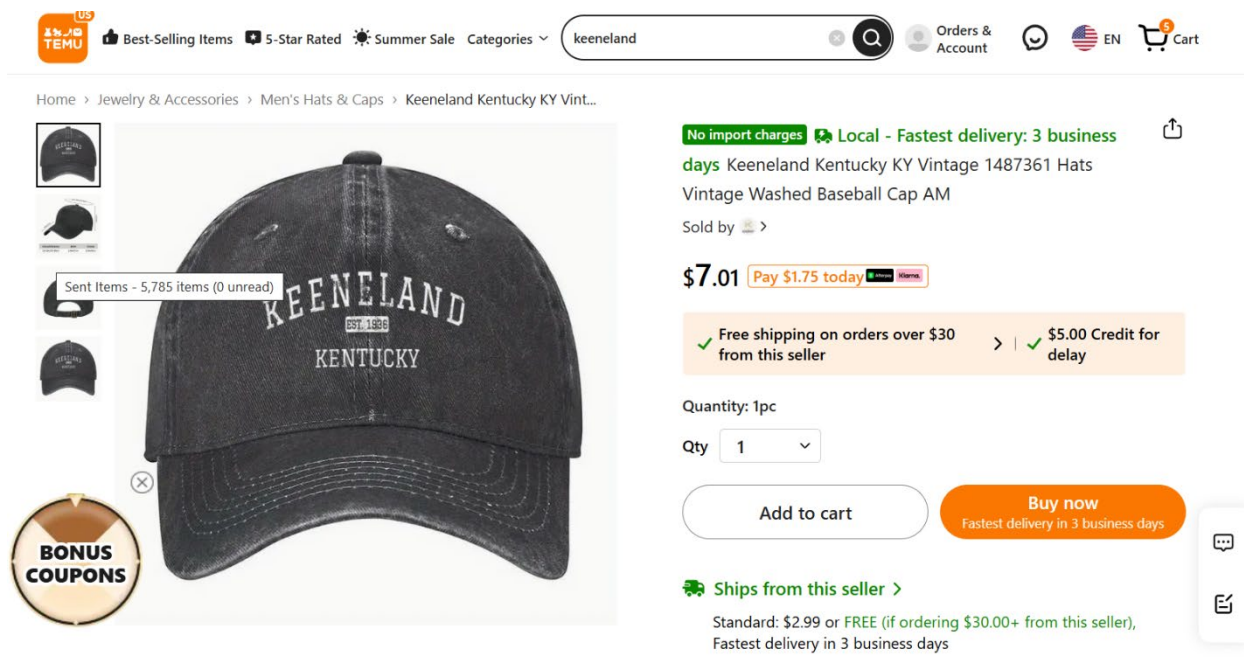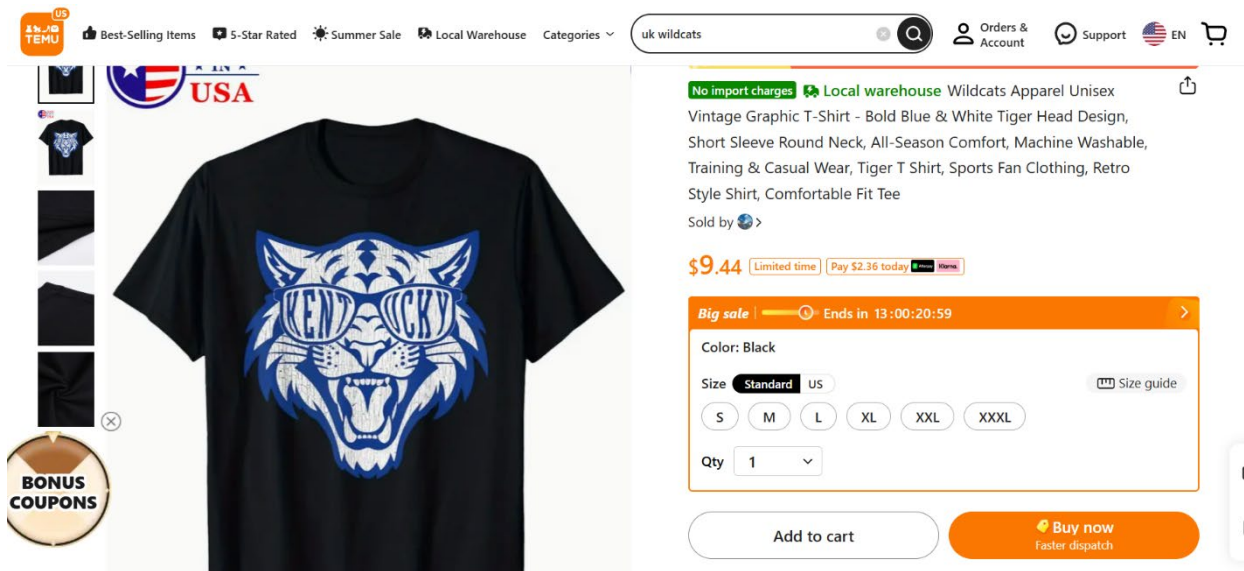**Figure 10: Temu product listing for a counterfeit "Vintage Buffalo Trace" sign.**

Figure 11: Temu product listing for a counterfeit "151ˢᵗ Kentucky Derby" t-shirt.

69

Figure 12: Temu product listing for a counterfeit "Keeneland" hat.

Figure 13: Temu product listing for a counterfeit "University of Kentucky Wildcats" t-shirt.
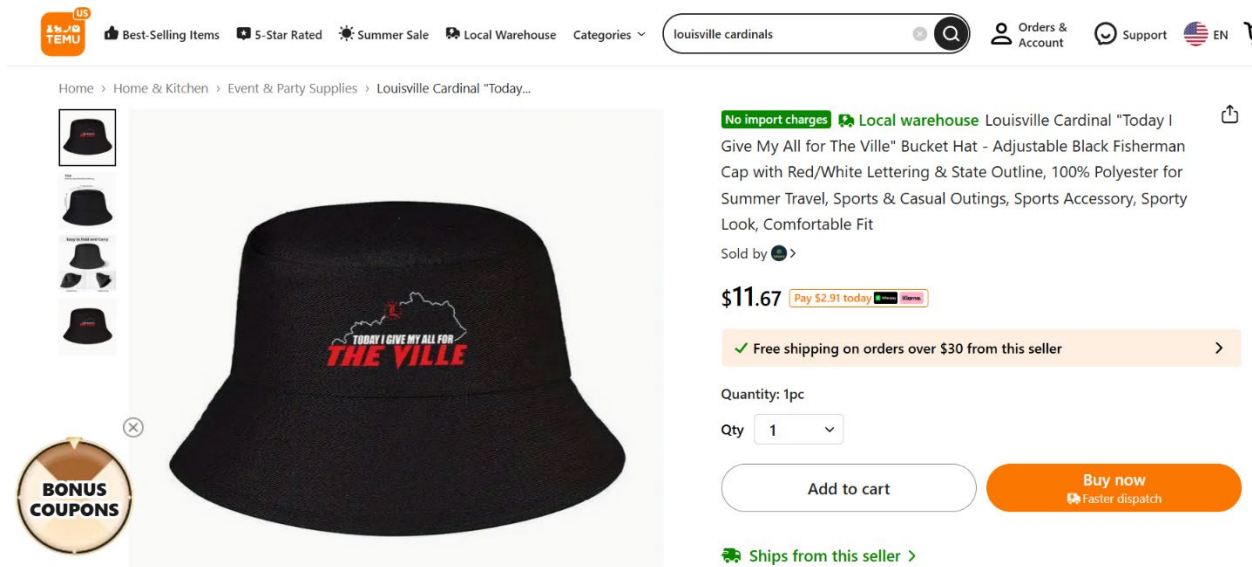
70

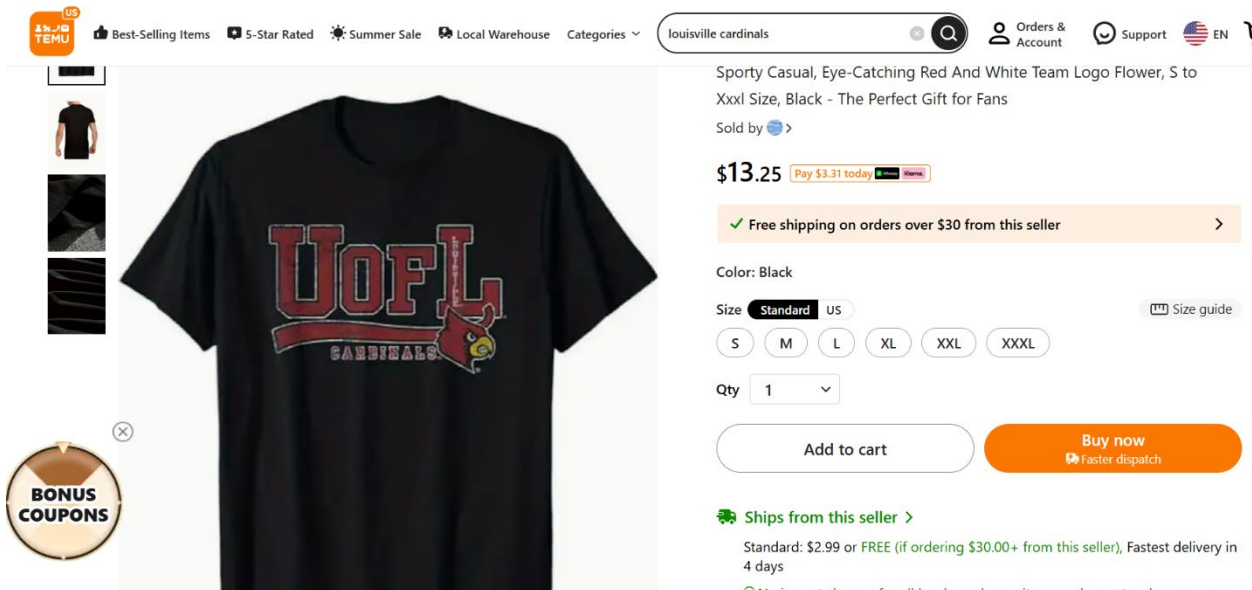**Figure 14: Temu product listing for a counterfeit "University of Louisville" hat.**

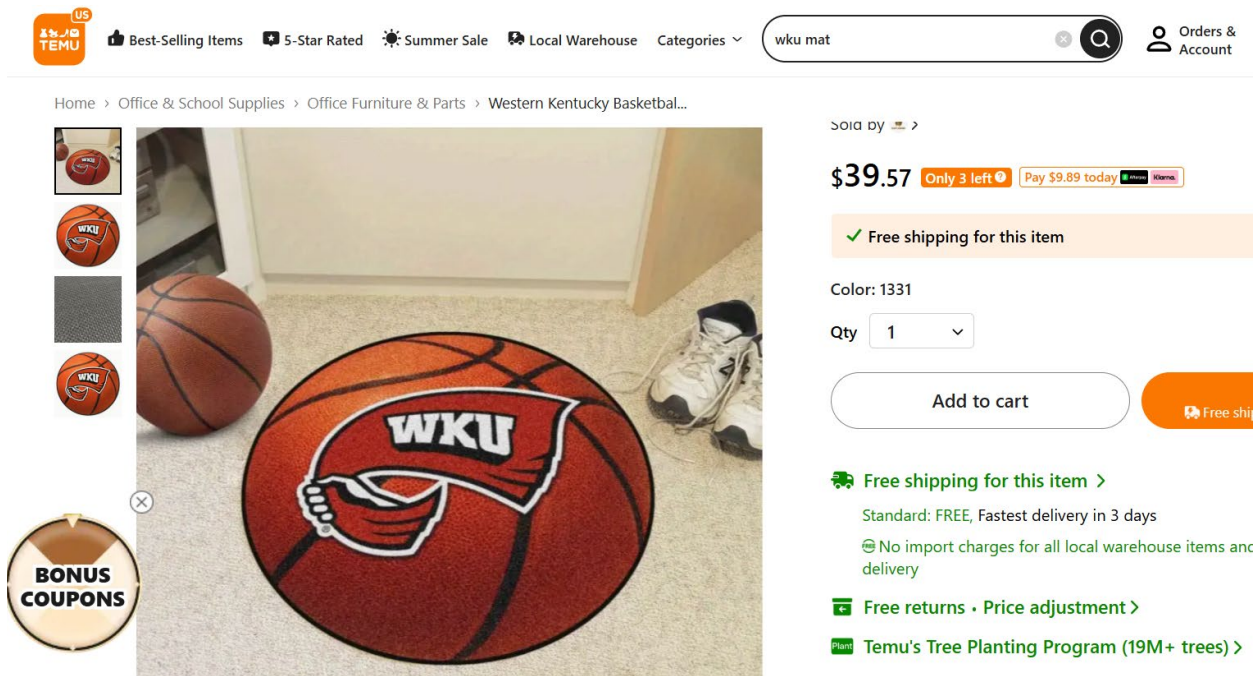**Figure 15: Temu product listing for a counterfeit "University of Louisville" t-shirt.**

71

Figure 16: Temu product listing for a counterfeit Western Kentucky University floor mat.
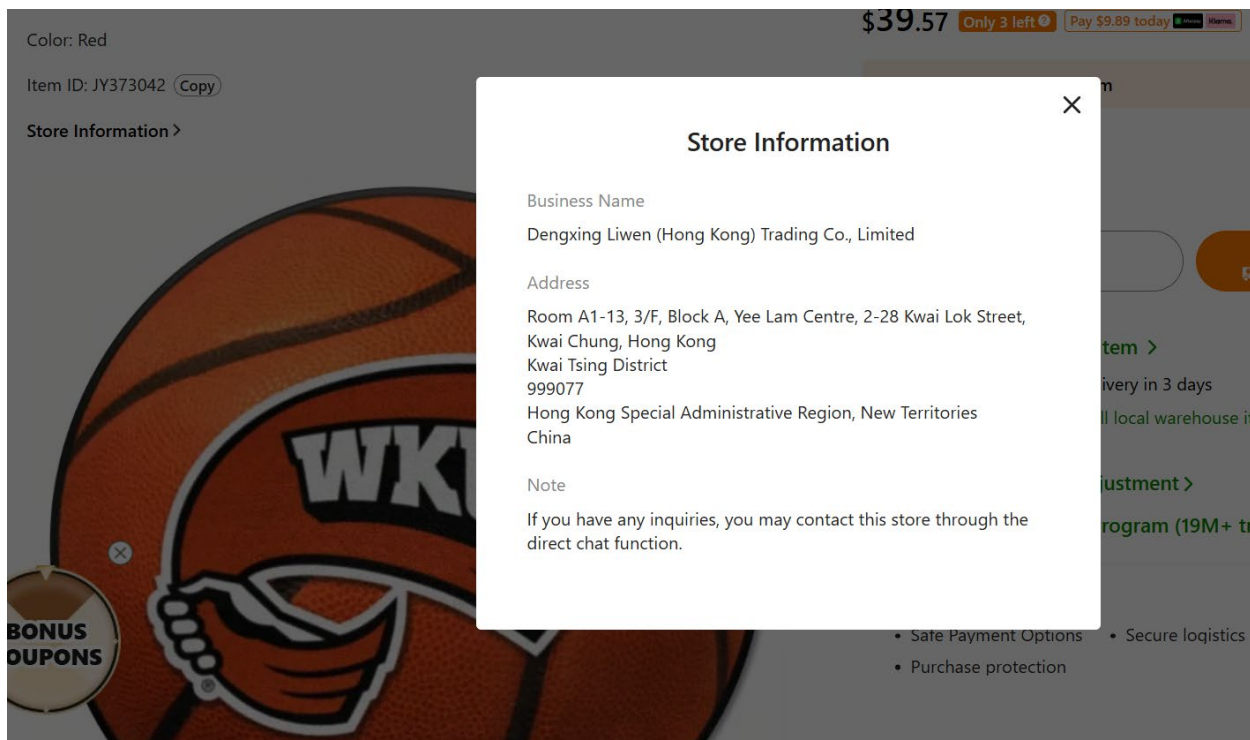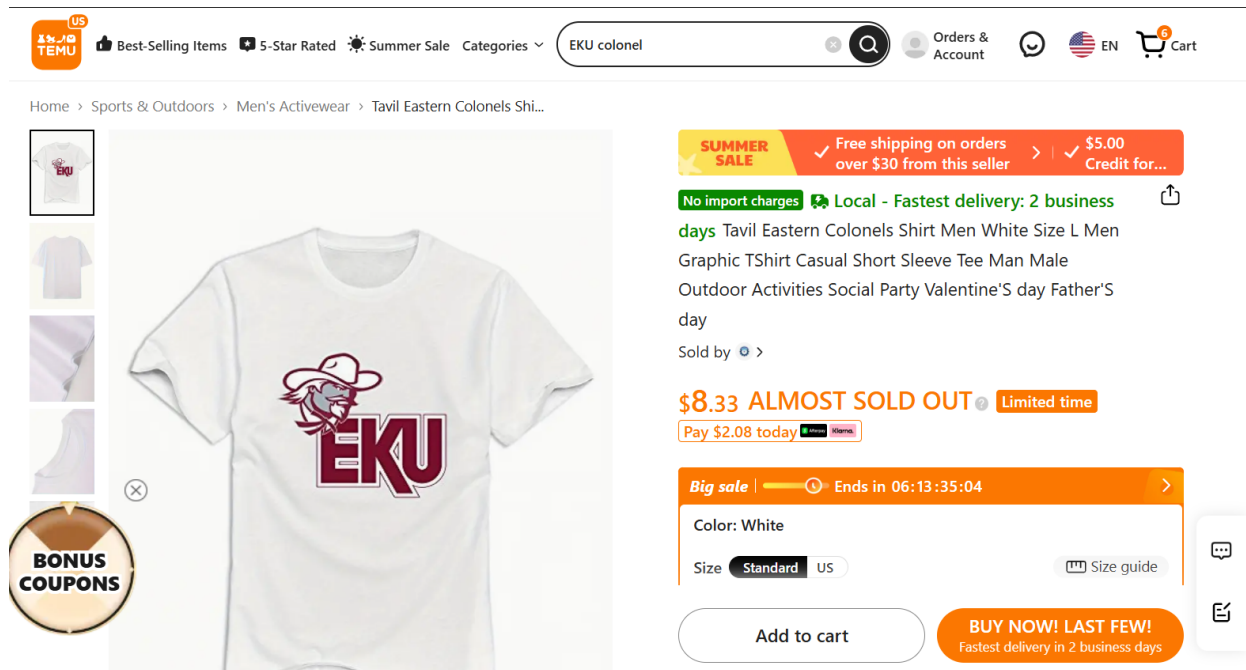

Figure 17: Store and origin information for counterfeit Wester Kentucky University floor mat.

Figure 18: Temu product listing for a counterfeit "EKU Colonels" t-shirt

227.   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 Unconscionable Dispute Resolution Process

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

229.   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.

230. 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.

231. 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).

232. 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*.

233. 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 KCPA.

x. "Greenwashing"

234. 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.

235.   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*."[127] (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.[128]

236.   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.

V.   CLAIMS

COUNT 1: UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN VIOLATION OF KENTUCKY CONSUMER PROTECTION ACT (KCPA) – PRIVACY HARMS (KRS 367.110 *ET SEQ.*)

237.   The Commonwealth of Kentucky re-alleges the facts above and incorporates them herein by reference.

---

[127] *Temu's Tree Planting Program*, Temu, https://www.temu.com/tree-landing.html (last visited June 6, 2025).
[128] *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.

238.   Defendants engaged in trade or commerce in the Commonwealth of Kentucky. Kentucky's Consumer Protection Act ("KCPA"), KRS 367.110 *et seq*., prohibits "[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce." KRS 367.170.

239.   Under KRS 367.190, "[w]henever the Attorney General has reason to believe that any person is using, has used, or is about to use any method, act or practice declared by KRS 367.170 to be unlawful, and that proceedings would be in the public interest," he may seek injunctive relief, and further may seek (i) a civil penalty of up to $25,000 per violation of any temporary or permanent injunction issued under KRS 367.190, and (ii) a civil penalty of up to $2,000 per willful violation of the KCPA. *See* KRS 367.990(1)-(2).

240.   As a result of Defendants' conduct as alleged herein, Kentucky citizens suffered and continue to suffer substantial injury.

241.   The unfair, false, misleading, and/or deceptive acts committed by Defendants constitute a breach of the duties enumerated under Kentucky law, including but not limited to the KCPA.

242.   **Unfair Practices:** Defendants' acts and practices were unfair under KRS 367.170. These unfair acts or practices include, but are not limited to, creating an app purported to be an e-commerce platform, which in reality is designed to collect users' PII in a manner that is unknown—and due to the intentional design of the Temu app—potentially unknowable to users. 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 Kentucky.

243.   The fact that the Temu app's privacy-violative conduct is executed through code—that is, in a manner that is invisible to the layperson—makes the conduct complained of all the

more egregious, as there is no way for Kentuckians to know the full extent of the nature of the privacy harms visited upon them by the app. Indeed, 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.

244.   **<u>False, Misleading, and/or Deceptive Acts</u>:** Defendants utilize deception—in the forms of misrepresentation, 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 an adversarial government.

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

246.   Defendants' acts and practices as alleged herein were motivated by a desire to retain and increase their profits.

247.   For each of Defendants' willful violations of KRS 367.170, the Commonwealth is entitled to recover a civil penalty of not more than two thousand dollars ($2,000) per violation, as well as all additional available relief, be it equitable (in the form of an injunction, declaratory, or other relief), or damages.

COUNT II: UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN VIOLATION OF KENTUCKY CONSUMER PROTECTION ACT – COMMERCIAL HARMS (KRS 367.110 *ET SEQ.*)

248.   The Commonwealth of Kentucky re-alleges the facts above and incorporates them herein by reference.

249.   Defendants engaged in trade or commerce in the Commonwealth of Kentucky.

250.   Kentucky's Consumer Protection Act ("KCPA"), KRS 367.110 *et seq*., prohibits "[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce." KRS 367.170.

251.   Under KRS 367.190, "[w]henever the Attorney General has reason to believe that any person is using, has used, or is about to use any method, act or practice declared by KRS 367.170 to be unlawful, and that proceedings would be in the public interest," he may seek injunctive relief.

252.   As a result of Defendants' conduct as alleged herein, Kentucky suffered and continues to suffer substantial injury.

253.   As described in Section J above, Defendants engaged in commercial-related deceptive acts or practices in violation of the KCPA.

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

255.   Defendants' acts and practices as alleged herein were motivated by a desire to retain and increase their profits.

256.   For each of Defendants' willful violations of KRS 367.170, the Commonwealth is entitled to recover a civil penalty of not more than two thousand dollars ($2,000) per violation, as well as all additional available relief, be it equitable (in the form of an injunction, declaratory, or other relief), or damages.

COUNT III: UNJUST ENRICHMENT

257.   The Commonwealth of Kentucky re-alleges the facts above and incorporates them herein by reference.

78

258.   The Commonwealth brings this Cause of Action for unjust enrichment against Defendants pursuant to its common law and/or *parens patriae* authority.

259.   As a direct and proximate result of the unlawful conduct described above, Defendants have been and will continue to be unjustly enriched.

260.   Defendants have benefited from their unlawful acts, realizing billions of dollars in revenues and profits through the unauthorized collection, accumulation, harvesting, use, and monetization of vast amounts of users' PII, as well as through its false, misleading, and or deceptive business practices vis-à-vis the goods sold on its platform and the representations, misrepresentations, and omissions related thereto.

261.   It would be inequitable and not in good conscience for Defendants to retain any ill-gotten gains earned as a result of the conduct alleged herein – gains that would not exist but for the victimization of consumers in the State of Kentucky.

262.   Defendants have retained this significant benefit despite their knowledge and understanding of the privacy and commercial harms described herein.

263.   Plaintiff requests an order from the Court compelling Defendants to disgorge proceeds that they unjustly received.

PRAYER FOR RELIEF

Wherefore, Plaintiff respectfully prays that the Court grant the following relief:

Entering an Order finding that the Defendants have violated the Kentucky Consumer Protection Act, as well as the common law of Kentucky as set forth herein, and have been unjustly enriched by such, and that judgment be entered against Defendants in favor of Plaintiff;

a.   Granting Plaintiff all recoverable measures of damages allowable under the claims identified herein;

Awarding Plaintiff penalties of up to $2,000.00 per violation of the KCPA;

b. Awarding Plaintiff disgorgement of all of Defendants' ill-gotten gains;

Entering an Order finding that, in accordance with the KCPA, Defendants, their affiliates, successors, transferees, assignees, and the officers, directors, partners, agents, and employees thereof, and all other persons acting or claiming to act on their behalf or in concert with them, be enjoined and restrained from in any manner continuing, maintaining or renewing the conduct, alleged herein in violation of the above stated Kentucky laws, or from entering into any other act, contract, or conspiracy having a similar purpose or effect;

Allowing Plaintiff to recover the costs and expenses of suit, pre- and post-judgment interest, and reasonable attorneys' fees as provided by law; and

Ordering such other and further relief as the Court deems just, necessary, and appropriate.

RESPECTFULLY SUBMITTED, this the 17th day of July, 2025.

RUSSELL COLEMAN
Attorney General
Commonwealth of Kentucky

J. Christian Lewis (KY Bar No. 87109)
Stephen B. Humphress (KY Bar No. 84880)
Lyndsey M. Antos (KY Bar No. 99971)
1024 Capital Center Drive, Suite 200
Frankfort, KY 40601
christian.lewis@ky.gov
steve.humphress@ky.gov
lyndsey.antos@ky.gov
Phone: (502) 696-5300
Fax: (502) 564-2698

Brian E. McMath, *pro hac pending*
Brian L. Moore, *pro hac 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 pending*
WADE KILPELA SLADE
1 Riverfront Place, Suite 745
North Little Rock, Arkansas 72114
slade@waykayslay.com

Attorneys for the Commonwealth of Kentucky

4D89E9CD-2C77-47C1-85D9-CB7C2E59A578 : 000081 of 000084

Presiding Judge: HON. KATHRYN GABHART (614428)

COM : 000081 of 000081

Commonwealth of Kentucky
Court of Justice   *Courts.ky.gov*

CR 4.02; Cr Official Form 1

CIVIL SUMMONS

Case #: **25-CI-00232**

Court: **CIRCUIT**

County: **WOODFORD**

Plantiff, **COMMONWEALTH OF KENTUCY VS. PDD HOLDINGS INC. ET AL**, *Defendant*

TO: **CORPORATION SERVICE COMPANY**

   421 WEST MAIN STREET

   FRANKFORT, KY 40601

Memo: Related party is WHALECO INC.

The Commonwealth of Kentucky to Defendant:
WHALECO INC.

   You are hereby notified that a **legal action has been filed against you** in this Court demanding relief as shown on the document delivered to you with this Summons. **Unless a written defense is made by you or by an attorney on your behalf within twenty (20) days** following the day this paper is delivered to you, judgment by default may be taken against you for the relief demanded in the attached complaint.

The name(s) and address(es) of the party or parties demanding relief against you or his/her (their) attorney(s) are shown on the document delivered to you with this Summons.

Sarah W. Sittrell

Woodford Circuit Clerk
Date: **7/17/2025**

Proof of Service

This Summons was:

☐ Served by delivering a true copy and the Complaint (or other initiating document)

   To: _____

☐ Not Served because: _____

   Date: _____, 20_____

   _____
   Served By

   _____
   Title

4D89E9CD-2C77-47C1-85D9-CB7C2E59A578 : 000082 of 000084

Presiding Judge: HON. KATHRYN GABHART (614428)

CI : 000001 of 000001

AOC-E-105   Sum Code: CI
Rev. 9-14

Commonwealth of Kentucky
Court of Justice   *Courts.ky.gov*

CR 4.02; Cr Official Form 1

COMMONWEALTH OF KENTUCKY
COURT OF JUSTICE

CIVIL SUMMONS

Case #: **25-CI-00232**

Court: **CIRCUIT**

County: **WOODFORD**

Plantiff, **COMMONWEALTH OF KENTUCY VS. PDD HOLDINGS INC. ET AL**, *Defendant*

TO: **PUGLISI & ASSOCIATES**
     850 LIBRARY AVE.
     SUITE 204
     NEWARK, DE 19711

Memo: Related party is PDD HOLDINGS INC.

The Commonwealth of Kentucky to Defendant:
PDD HOLDINGS INC.

   You are hereby notified that a **legal action has been filed against you** in this Court demanding relief as shown on the document delivered to you with this Summons. **Unless a written defense is made by you or by an attorney on your behalf within twenty (20) days** following the day this paper is delivered to you, judgment by default may be taken against you for the relief demanded in the attached complaint.

The name(s) and address(es) of the party or parties demanding relief against you or his/her (their) attorney(s) are shown on the document delivered to you with this Summons.

Sarah W. Fittrell
Woodford Circuit Clerk
Date: **7/17/2025**

Proof of Service

This Summons was:

☐ Served by delivering a true copy and the Complaint (or other initiating document)

   To: _____

☐ Not Served because: _____

Date: _____, 20_____

_____
Served By

_____
Title

Summons ID: @90005843302
CIRCUIT: 25-CI-00232 Certified Mail
COMMONWEALTH OF KENTUCKY VS. PDD HOLDINGS INC. ET AL

Page 1 of 1

eFiled

Commonwealth of Kentucky
Sarah Littrell, Woodford Circuit Clerk

Case #: 25-CI-00232	**Envelope #:** 11096595
Received From: CHRIS LEWIS	**Account Of:** CHRIS LEWIS
Case Title: COMMONWEALTH OF KENTUCY VS. PDD HOLDINGS INC, ET AL	**Confirmation Number:** commonwealth
Filed On 7/17/2025 10:50:23AM	

#	Item Description	Amount
1	Court Facilities Fee	$25.00
2	Court Facilities Fee	-$25.00
3	Access To Justice Fee	-$20.00
4	Access To Justice Fee	$20.00
5	Money Collected For Others(Court Tech. Fee)	$20.00
6	Money Collected For Others(Court Tech. Fee)	-$20.00
7	Money Collected For Others(Postage)	$58.20
8	Money Collected For Others(Postage)	-$58.20
9	Money Collected For Others(Attorney Tax Fee)	$5.00
10	Money Collected For Others(Attorney Tax Fee)	-$5.00
11	Library Fee	-$1.00
12	Library Fee	$1.00
13	Civil Filing Fee	$150.00
14	Civil Filing Fee	-$150.00
15	Charges For Services(Copy - Photocopy)	-$16.60
16	Charges For Services(Copy - Photocopy)	$16.60
17	Charges For Services(Jury Demand / 12)	$70.00
18	Charges For Services(Jury Demand / 12)	-$70.00
	TOTAL:	$0.00