IN THE IOWA DISTRICT COURT FOR POLK COUNTY

STATE OF IOWA, *ex rel.* ATTORNEY GENERAL BRENNA BIRD, Plaintiff, v. **PDD HOLDINGS, INC., F/K/A PINDUODUO INC.;** AND **WHALECO, INC., (D/B/A TEMU)**, Defendants.	Equity No. _____ **PETITION**

TABLE OF CONTENTS

I. INTRODUCTION 1

A. Overview of Temu 3

B. Overview of Privacy Harms Caused by the Temu App 5

C. Overview of Commercial Harms Endemic to Temu 9

II. JURISDICTION AND VENUE 9

III. PARTIES 11

A. The State of Iowa 11

B. PDD Holdings Inc., f/k/a Pinduoduo Inc. 11

C. Whaleco Inc., d/b/a Temu 12

D. Temu Payments Inc 12

E. Alter Ego and Single Enterprise Allegations 12

IV. GENERAL FACTUAL ALLEGATIONS 14

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. 14

B. The Pinduoduo App Has Been Deemed to Be Malware by Security Experts and Was Banned from Google's App Marketplace. 15

C. In 2022, PDD Holdings Developed the Temu App, Which is Modeled on Pinduoduo—Including Through Its Design and Code—and Which Defendants Aggressively Marketed in the United States and Iowa. 18

V. TEMU'S PRIVACY HARMS 19

A. Precisely Like the Pinduoduo App, Defendants' Temu App Presents a Host of Undisclosed Privacy and Security Risks 19

1. Excessive, Unjustifiable, and Hidden Collection of Users' PII 21

2. Design and Programming That Intentionally Evades Scrutiny 28

3. Overlap with Pinduoduo Code 35

B. Users Do Not Consent to Defendants' Data Collection Practices. 36

C. Defendants Are Violating Iowans' Right to Privacy of Their Data 43

D. Defendants Have Collected Personal Information from Minors, Including Minors Under the Age of Thirteen 47

E. Temu Subjects User Data to Misappropriation by Chinese Authorities 49

F. Defendants Acknowledge That They Risk Being Subject to China's Laws Regarding User's Data in Their Possession 57

VI. TEMU's COMMERCIAL HARMS 58

A. Defendants Also Engage in Deceptive and Unfair Trade Practices in the Offer and Sale of Products on the Temu App and the Resolution of Consumer Complaints. 58

1. Deceptive Representations as to the Quality of Goods 60
2. Pricing Misrepresentations 61
3. Charges for Goods Not Ordered or Not Delivered 62
4. Sign-Up Scams, Gamification, Store Credit, and Failure to Honor Terms 63
5. Fake Reviews 67
6. Intellectual Property Theft 68
7. Use of Forced Labor 74
8. "Greenwashing" 76

VII. CAUSES OF ACTION 78

A. Claims Under the Consumer Fraud Act and Civil Penalties 78

1. Privacy Harms 78
2. Commercial Harms 79
3. Reimbursement and Disgorgement 80

VIII. PRAYER FOR RELIEF 81

I. INTRODUCTION

1. Under the guise of the ability for everyday Iowans to "shop like a billionaire," Temu and its shopping app deceptively harvests data from Iowans and provides a pathway for that harvested data to flow to China. It does that while committing numerous consumer frauds such as false representations about the quality of goods, sign-up scams, pricing misrepresentations, and many more. For the cherry on top, Temu shows a lack of regard for intellectual property rights, including those of the University of Iowa regarding its Hawkeyes' gear and even of the IOWA Wave, where proceeds benefit pediatric cancer and illness research.

2. Temu is a shopping app with ties to China that covertly collects a substantial amount of personal data about Iowa consumers, well beyond what is necessary for a shopping app.

3. Temu deceives Iowa consumers about its data-collection practices, engineering its app in a manner that is meant to hide its data exfiltration, and further making demonstrably false representations and engaging in material omissions as to its privacy-invasive conduct.

4. Moreover, Temu deceives Iowans about the quality of the products offered on its platform, flooding the United States and Iowa markets with substandard products. Temu also uses false reference pricing, gamification, and unlicensed items that violate intellectual property rights to entice consumers to spend more time on the app so it can collect more data about Iowa consumers. As a result, Temu further violates Iowans' privacy rights, and causes them financial harms.

5. The harms committed against Iowa by Defendants are multifold. This Petition challenges Defendants' many acts and practices that are unlawful under the Iowa Consumer Fraud Act (the "CFA").

6. Section V of this Petition (¶¶ 82–212) discusses harms to Iowans and violations of the CFA that involve threats to Iowans' privacy and security due to code-level behaviors in the Temu app which the State's expert investigation has uncovered.

7. 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 alone is a violation of the CFA, this additional geopolitical component amplifies the consequences of that existing violation.

8. Section VI of the Petition (¶¶ 213–64) discusses harms to Iowans and violations of the CFA that involve misrepresentations as to the quality of goods, pricing misrepresentations, sign up scams, failure to honor terms, greenwashing and more. Temu sells products to Iowans in ways that are plainly violative of the CFA.

9. The State of Iowa brings this case to redress and restrain violations of the CFA. The State seeks a preliminary and permanent injunction under the CFA to compel Defendants to stop their conduct challenged herein. The State also seeks reimbursement, civil penalties, and any other equitable relief to which the State is entitled, including, but not limited to, disgorgement of all moneys or property acquired by Defendants' from their unlawful behavior.

A. Overview of Temu

10. 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.

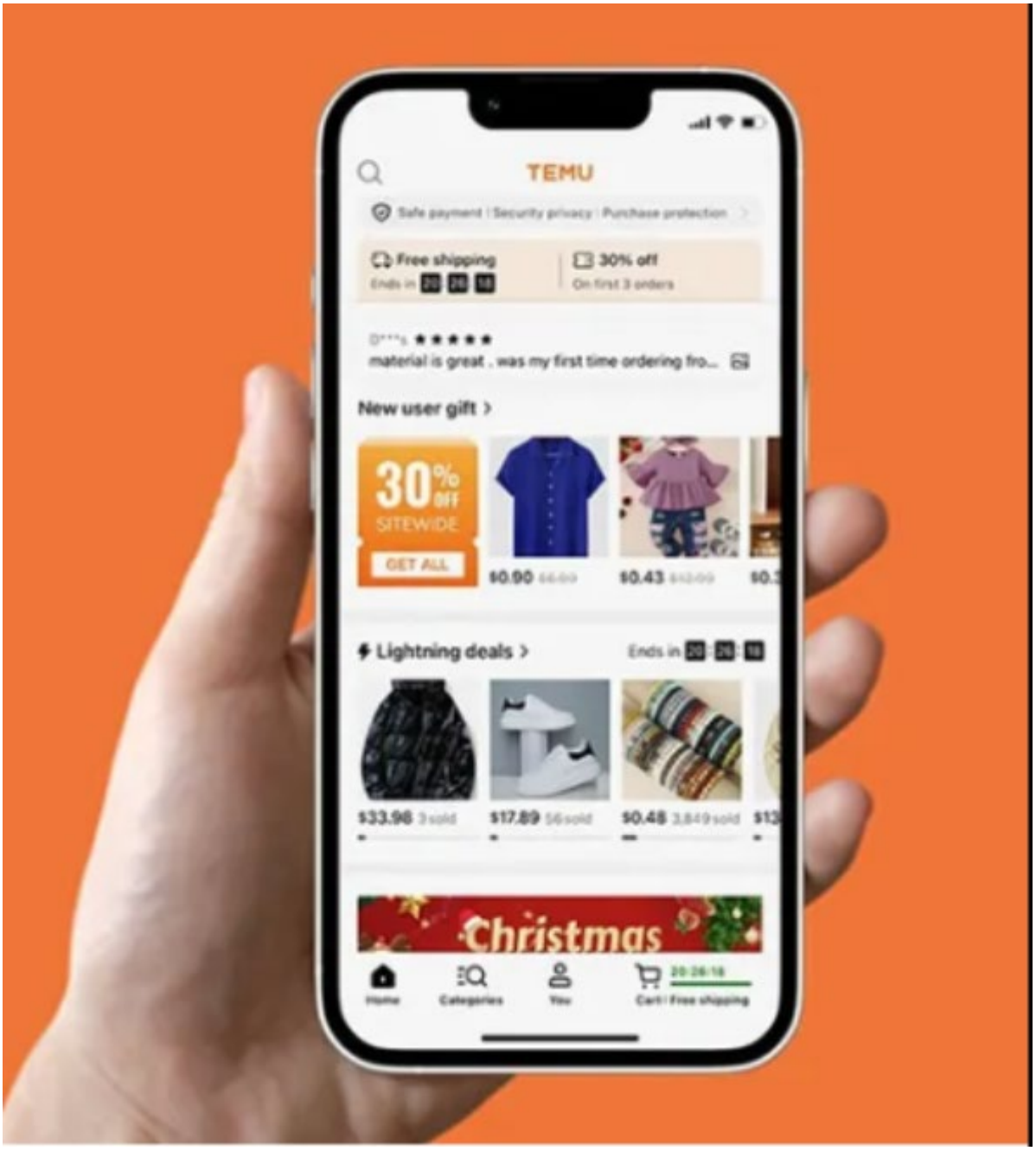

Figure 1: Representation of the Temu mobile application.

11. 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.

13. The Temu app is wildly popular throughout the United States, including in the State of Iowa, with usage driven both via word of mouth and by an aggressive, multibillion-dollar

marketing campaign. This campaign made headlines for three separate advertisements that Temu aired during the 2024 Super Bowl, as well as two additional advertisements aired immediately following the game.[1] The advertisements "featured animated characters using the app to transform their lives to the tune of a catchy jingle. The marketing campaign urged viewers…to 'shop like a billionaire' as the ad's avatars filled their homes with $10 toasters and $6 skateboards."[2]

14. 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]

B. Overview of Privacy Harms Caused by the Temu App

15. But Temu is more than an e-commerce platform—it is a data siphoning juggernaut. Disturbingly, a host of security and privacy concerns have been raised about both the Temu app and its precursor, the Pinduoduo app.

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

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

[2] *Id*.

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

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

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

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

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

18. Iowa has consulted and retained expert forensic investigators who have examined the code of the Temu app and its predecessor, the Pinduoduo app, and focused on the ways in which each app has code and functionality overlap.

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

20. Except where specifically noted, all factual allegations in this Petition about the technical design, functionality, and features of the Temu app are based on Iowa's retained expert forensic investigation and do not rely or depend on any outside forensic analysis.

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

---

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

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

23. 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.

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

25. These privacy and security risks and harms 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.[7] This mandate to Chinese

[7] *Safeguarding Our Future — U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies*, Nat'l Counterintelligence & Sec. Ctr. (June 23, 2023), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

organizations and citizens is "secret" because Chinese law not only imposes a duty on Chinese organizations and citizens to cooperate with the Chinese intelligence apparatus, but also to "protect the secrecy of any state intelligence work secrets of which they are aware."[8]

26. The sensitive PII that Temu collects from Iowa 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.

27. 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 Iowa users is being sent to and used by the Chinese government.

28. 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.

29. For example, in 2023, the State of Montana 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.[9]

30. Likewise, Defendants are currently the subject of a congressional investigation based on "concerns about Temu and the amount of data collected."[10]

---

[8] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017, 11:30 AM) (quotation marks omitted), https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense.

[9] 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.

[10] Letter from Cathy McMorris Rodgers & Gus M. Bilirakis, U.S. Cong. Comm. on Energy & Commerce, to Mr. Qin Sun, President of Whaleco, Inc. d/b/a Temu and Pinduoduo (Dec. 20, 2023),

31. 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.

C. Overview of Commercial Harms Endemic to Temu

32. 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.[11] As of the date of this filing, Temu features dozens of what appear to be unlicensed products claiming to be from Iowa brands like the University of Iowa (and the Hawkeye wave), Art's Way, and Dowling Catholic.

33. Accordingly, the State brings this part of the action under the CFA and seeks a permanent injunction preventing Defendants from acquiring, maintaining, and otherwise utilizing the PII of Iowa citizens, preventing Defendants from allowing widespread intellectual property infringement to the detriment and confusion of Iowa consumers, and Attorney General Bird further seeks reimbursement, disgorgement, and civil penalties in light of Defendants' conduct, as well as all other available relief allowed by law.

II. JURISDICTION AND VENUE

34. The Attorney General, as Iowa's Chief Law Enforcement Officer, is expressly authorized to enforce the CFA under Iowa Code § 714.16(7), and this Court has subject-matter jurisdiction over this matter under Iowa Code § 714.16(7).

---

https://d1dth6e84htgma.cloudfront.net/CCP_Marketplace_Letter_to_Whaleco_Inc_Temu_7f921e1a67.pdf.

[11] 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/.

35. This Court has personal jurisdiction over the Defendants because of their contacts in Iowa. Defendants conduct business in Iowa and have purposefully availed themselves of this forum by conducting business in the State and by causing harm as a direct and proximate result of their actions.

36. At all relevant times, the Defendants regularly transacted or solicited business in the State and derived substantial revenue from goods used or consumed or services rendered in the State or contracted to supply goods or services in the State and either caused injury by an act or omission in the State or caused injury in the State by an act or omission outside the State.

37. At all times relevant to this Petition, Defendants have operated the Temu app which has been intentionally directed towards, marketed to, and downloaded by citizens of the State. Defendants have engaged in myriad commercial transactions with Iowa consumers, taking payment from consumers in Iowa-based commercial transactions and sending various products to Iowa consumers. Defendants have also sold goods to consumers purporting to be authentic or licensed by a multitude of Iowa-based businesses and institutions, including but not limited to the University of Iowa (and the Hawkeye Wave), Art's Way, and Dowling Catholic.

38. Defendants were—and remain—in possession of and/or have or have had control over sensitive PII of Iowa citizens. Defendants have the requisite minimum contacts with Iowa necessary to permit this Court to exercise jurisdiction.

39. Furthermore, Defendants have a registered agent in Iowa, Temu Payments, Inc.

40. The conduct described in this Petition arises from Temu's purposeful directed activities to Iowa and Temu consumers in Iowa.

41. On information and belief, Polk County is a proper venue because it is a "county where the transaction or any substantial part of the transaction occurred" and because it is "where one or more of the victims reside" Iowa Code § 714.16(10).

III. PARTIES

A. The State of Iowa

42. Plaintiff is the State of Iowa, *ex rel.* Brenna Bird, Attorney General of Iowa. Under Iowa Code § 714.16(7), the Attorney General may seek civil enforcement of the Iowa Consumer Fraud Act. The Attorney General brings this action on behalf of the people of the State of Iowa to protect the state and its residents from Defendants' unlawful business practices.

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

43. Defendant PDD Holdings Inc. ("PDD Holdings") was founded in China in 2015 under the name Pinduoduo, and is registered in the Cayman Islands. It owns and operates a portfolio of businesses both in China and the United States. Among other things, PDD Holdings owns and operates the Pinduoduo e-commerce platform that offers various consumer products. PDD Holdings also owns the company that operates the Temu online marketplace (Co-Defendant Whaleco, Inc., discussed *infra*). PDD Holdings was formerly known as Pinduoduo Inc., with headquarters in Shanghai, China. In February 2023, PDD Holdings moved its "principal executive offices" from Shanghai, China to Dublin, Ireland.[12] However, it continues to have significant operations in China, with multiple subsidiaries located within that country.

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

[12] 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.

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

45. 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. Temu Payments Inc.

46. Temu Payments Inc. ("TPI") is a foreign for-profit corporation incorporated in November 2024, which maintains a registered agent in Des Moines. TPI also maintains its principal place of business at 31 James Ave., Suite 355, Boston, MA, 02116, the very same address as Defendant Whaleco. On information and belief, TPI serves as a money transmitter and payment processor for Temu within the State of Iowa.

E. Alter Ego and Single Enterprise Allegations

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

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

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

50. Defendant PDD Holdings' 2024 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 consumers and growing sales."[13]

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

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

53. Defendants' Temu app contains significant code overlap with Defendants' Pinduoduo app, including proprietary code and app programming components copied directly from the Pinduoduo app into the Temu app that are central to Defendants' violation of the Iowa Consumer Fraud Act discussed *infra* at paragraphs 150–54.

54. 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.

55. 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

[13] PDD Holdings, Form 20-F Annual Report (2024), https://www.sec.gov/Archives/edgar/data/1737806/000141057825000951/pdd-20241231x20f.htm.

below, each Defendant is also directly liable based on its own actions independent of any alter ego or single enterprise theory of liability.

IV. GENERAL FACTUAL ALLEGATIONS

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.

56. 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.[14]

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

58. 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."[15]

[14] 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.

[15] PDD Holdings, Form 20-F Annual Report (2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/1737806/000110465923049927/pdd-20221231x20f.htm.

59. 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,[16] thus incentivizing the proliferation of the app on social media platforms.

60. 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.

61. On March 21, 2023, Google suspended the Pinduoduo app from the Google Play Store after malware issues were found on the app.[17] 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."[18]

---

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

[17] 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/.

[18] Nectar Gan, et al., *'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.

62. 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.[19]

63. 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."[20]

64. 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."[21] The purpose of this was, "to spy on users and competitors, allegedly to boost sales,"[22] according to a company insider.

65. 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.[23]

66. 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."[24]

---

[19] *Id.*
[20] *Id.*
[21] 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.
[22] *Id.*
[23] Gan, *et al.*, *supra* note 18.
[24] *Id.*

67. According to a company insider source, who requested anonymity for fear of reprisals, "[t]he goal was to reduce the risk of being exposed."[25]

68. This bears repeating: Pinduoduo hired a small army to figure out vulnerabilities in the Android operating system and then use those discovered vulnerabilities to secretly acquire users' PII in contravention of safeguards that Android had established. As discussed in paragraphs 148 through 154, *infra*, the work of this group continues to manifest itself in Temu, as well.

69. Moreover, once the app was installed, the app was able to continue running in the background and prevent itself from being uninstalled.[26]

70. One security researcher interviewed by CNN described Pinduoduo as "the most dangerous malware ever found among mainstream apps."[27]

71. 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.

72. 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.

[25] *Id.*
[26] *Id.*
[27] *Id.*

73. 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."[28]

74. 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.[29]

75. Thereafter, most of the members on this team were transferred to work at Temu.[30]

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

76. 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.[31]

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

78. 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.[32]

79. 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,

[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] Goujard, *supra* note 6.
[32] Gan, *et al.*, *supra* note 18.

payment processing, and after-sales services for merchants on its platform. "Temu's network now includes more than 80,000 suppliers."[33]

80. 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.[34] As a result, the market capitalization of Defendant PDD Holdings swelled to nearly $185 billion as of September 23, 2025.[35]

81. 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 Iowa—through Temu's network of more than 80,000 China-based sellers participating in its online marketplace.[36]

V. TEMU'S PRIVACY HARMS

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

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

83. This conduct came to light following the removal of the Pinduoduo app from Google's Play Store on March 21, 2023. In a public statement released that day, Google explained that "[w]e have suspended the Play version of the [Pinduoduo] app for security concerns," and that

[33] Staff of H.R. Select Comm. on the CCP, 118th Cong., *Report on Fast Fashion and the Uyghur Genocide: Interim Findings* at 4 (2023), https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf.
[34] Perez, *supra* note 3.
[35] Nasdaq GS, *PDD Holdings Inc. (PDD)*, Yahoo!Finance, https://finance.yahoo.com/quote/PDD/ (last visited June 23, 2026).
[36] Staff of H.R. Select Comm. on the CCP, *supra* note 33, at 8.

Google Play "has been set to block installation attempts. . . . Users that have malicious versions of the app downloaded to their devices are warned and prompted to uninstall the app."[37]

84. Google arrived at its conclusion to remove Pinduoduo 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*.

85. 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 be tracked on the internet [which is an option that all apps in Apple's online marketplace are required to provide to users]."[38]

86. As one commentator observed following the State of Montana's decision to ban the Temu app on government devices, 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."[39]

---

[37] Nectar Gan, *et al.*, *Google suspends Chinese shopping app Pinduoduo over malware*, CNN Business (Mar. 21, 2023, 8:06 AM), https://edition.cnn.com/2023/03/21/tech/china-google-pinduoduo-malware-app-intl-hk#:~:text=check%20back%20later.-,Google%20suspends%20Chinese%20shopping%20app%20Pinduoduo%20over%20malware,app%2C%E2%80%9D%20the%20spokesperson%20said.

[38] Goujard, *supra* note 6.

[39] Basilan, *supra* note 9.

87. Iowa's retained expert forensic investigation of the Temu app reveals a host of troubling conduct, including but not limited to the following:

a. The app allows for extensive data exfiltration from all corners of a user's mobile device.

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

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

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

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

89. These concerns are addressed more fully as follows:

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

90. Temu is designed to access and control virtually all aspects of a user's device, in furtherance of surreptitiously acquiring the sensitive PII contained therein. Iowa's retained expert forensic investigation reveals that, among other bad conduct, Temu acquires the following sensitive PII without user knowledge or consent—and often in direct contravention of Temu's representations to consumers.

i. Users' granular location data

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

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

93. Many of the data points Temu continued to acquire and which allowed it to determine precise location without formally including the ACCESS_FINE_LOCATION permission are discussed in paragraphs 94 through 96 and 114 through 118, *infra*.

ii. WiFi access points

94. 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.

95. 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.

96. 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)."[40]

iii. Microphone and camera access

97. Two permissions that Temu includes in its app are requests for CAMERA and RECORD_AUDIO, surreptitiously granting the app access to all of the audio and visual recording and storage functions of a user's device. These permissions are not adequately disclosed to users, as described in paragraphs 155 through 158, *infra*.

iv. Intentional Android exploit: ActivityManager.getRunningTasks

98. 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).[41]

99. 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,[42] 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

[40] 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.

[41] 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/.

[42] 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.

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.

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

101. 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* ¶¶ 138–39, *infra*.

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

102. Android Developer documentation explains that the method android.telephony.TelephonyManager.listen() "[p]rovides access to information about the telephony services on the device. Applications can use [these] methods to determine telephony services and states, as well as to access some types of subscriber information. Applications can also register a listener to receive notification of telephony state changes."[43]

103. 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.).

[43] Android, *TelephonyManager*, Developers—Guides, https://developer.android.com/reference/android/telephony/TelephonyManager (last updated Feb. 26, 2026).

104. 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.[44]

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

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

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

107. 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.

108. 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.

[44] 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 (Jan. 2021).

109. 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.[45]

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

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

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

111. 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."[46]

112. 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."[47]

---

[45] As explained in paragraphs 63–64, *supra*, the purpose of this data collection was done by Defendants in order "to spy on users and competitors, allegedly to boost sales."

[46] Android, *Manifest.permission*, Developers—Guides, https://developer.android.com/reference/android/Manifest.permission#GET_ACCOUNTS (last updated Feb. 26, 2026).

[47] Android, *AccountManager*, Developers—Guides, https://developer.android.com/reference/android/accounts/AccountManager (last updated Feb. 26, 2026).

113. 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.

viii. Additional sensitive PII

114. Temu also collects a host of other discrete PII generated by the user's device, which is universally recognized as individually-identifying pieces of information that can be—and routinely are—used to track, monitor, and profile individuals. That PII includes the following items listed in paragraphs 115 through 118, *infra:*

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

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

117. **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.[48]

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

2. Design and Programming That Intentionally Evades Scrutiny

i. Dynamic recompilation using the "Manwe" tool

119. 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.

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

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

[48] 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/.

122. 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.

123. Since Manwe allows Temu to evade Google's and Apple's security and privacy tests by enabling updates outside the app store's vetting process, 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.

124. 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.

125. And, as noted below, Temu also borrowed code from Pinduoduo in the form of the ZipPatch library (*see* ¶ 153, *infra*), which also allows the app to update its code without pushing the update through Google or Apple.

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

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

127. A manifest file is required for every app,[49] and *must* contain certain information, including the "permissions that the app needs in order to access protected parts of the system or other apps."[50] As Google explains on its webpage for Android developers, "Android apps must request permission to access sensitive user data, such as contacts and [text messages], or certain

[49] Android, *App manifest overview*, Developers – Guides, https://developer.android.com/guide/topics/manifest/manifest-intro (last updated Mar. 18, 2026).
[50] *Id.*

system features, such as the camera and internet access. Each permission is identified by a unique label."[51]

128. 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.

129. 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 Android manifest. An app's Android manifest is an XML file that every Android app has, and which is meant to act as a blueprint for that app, declaring to the reader how the app is intended to work.[52] Critically, Android manifests are the "foremost" data point relied upon by security researchers when conducting a static analysis (that is, code-level analysis) of a given app.[53] This is because they are supposed to give a high level overview of essential information about the app—most notably for purposes of this action, how the app is and is not supposed to behave on a user's device.

130. Among other things, the manifest must disclose any permissions it needs in order to access protected parts of a user's device. Thus, editing the manifest to remove the permissions ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION leads anyone reviewing the manifest to conclude that Temu was *not* collecting location data from its users.

---

[51] *Id.*
[52] *Id.*
[53] Lucideus, *Security Review of Android Manifest File -Part I*, Medium (Dec. 26, 2018), https://medium.com/@lucideus/security-review-of-android-manifest-file-part-i-ecb5ca51eb6a.

131. 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* ¶¶ 91–96, *supra*.

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

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

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

134. 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.

iv. Detection of "root" access on a device

135. 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.

136. More important to this Petition, 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. Thus, when an app tries to determine whether the device it is installed on has root access, it typically is trying to determine whether the app is being used in a "testing" environment.[54] If the app—like Temu—determines that a device has root access, it can surmise that someone is looking into the app's code. In turn, this enables the app to hide any behaviors or functions that it does not want discovered.

137. Iowa's retained expert forensic investigation has directly encountered this particular security countermeasure tool in the course of its own forensic investigation of the Temu app.

v. Searching for "debuggers"

138. 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.[55]

---

[54] *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 23, 2026).

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

139. 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.

vi. Code obfuscation

140. 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."[56]

141. 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.

142. 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.

vii. Heavily-encrypted network traffic

143. 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."

144. 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.

[56] *What is code obfuscation and how does it work?*, Guardsquare, https://www.guardsquare.com/what-is-code-obfuscation (last visited June 23, 2026).

145. 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.

146. 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.

147. 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.

148. 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.

149. Iowa's retained expert forensic 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. Iowa's expert 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.

3. Overlap with Pinduoduo Code

150. 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:

i. Package name overlap

151. 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.

ii. Specific code overlap

152. 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.

153. 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.

iii. SDK overlap

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

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

155. 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.

156. This is all the more egregious given that Defendants have issued 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."[57]

[57] 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.

157. 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.

158. 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* ¶ 16, *supra*.

159. 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 Petition hidden from its users.

October 17, 2022[58]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 97)	No mention of seeking microphone access (or of audio, generally)
Camera Access (¶ 97)	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."

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

Location Data (¶¶ 91–96, 114–17, 129–33)	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 (¶¶ 94–96)	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 (¶¶ 98–113)	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 (¶¶ 102–05)	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 (¶¶ 106–10)	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 (¶¶ 114–18)	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[59]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 97)	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 (¶ 97)	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."

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

Location Data (¶¶ 91–96, 114–17, 129–33)	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 (¶¶ 94–96)	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 (¶¶ 98–113)	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 (¶¶ 102–05)	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 (¶¶ 106–10)	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 (¶¶ 114–18)	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)[.]"

160. 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.

161. 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[60]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 97)	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 app/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 (¶ 97)	Temu removed its prior language quoted above and now says the following: "What Information 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 (¶¶ 91–96, 114–17, 129–33)	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 (¶¶ 94–96)	Temu removed its prior language quoted above and has not provided substitute language.

[60] *Privacy Policy*, Temu (May 12, 2025), https://web.archive.org/web/20250513155620/https://www.temu.com/privacy-and-cookie-policy.html.

User's Activity on His or Her Device, Outside of Temu (¶¶ 98–113)	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: … 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 (¶¶ 102–05)	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 (¶¶ 106–10)	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 (¶¶ 114–18)	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.

C. Defendants Are Violating Iowans' Right to Privacy of Their Data

162. 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.

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

164. Iowans 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.

165. "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 "a 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 (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.").

166. 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).

167. 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).

168. 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 "[c]urrent 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*, 516 F. Supp. 3d 1293 (D.N.M. 2021).

169. It is precisely because of Defendants' capacity for "near perfect surveillance" that Iowa 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*.

170. As discussed above, Defendants have designed the Temu app to surreptitiously 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.

171. 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 or permission.

172. 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."[61] 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.

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

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

173. 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.

174. 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.

175. 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.

176. 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.[62] Likewise, a consumer group in the United Kingdom found that Temu was selling age-restricted

[62] *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.

weapons such as survival knives and axes that were illegal for children to possess without any age verification.[63] Others have observed that Temu is filled with smoking and drug paraphernalia that is sold to any customer, without age verification.

177. Finally, Temu ran an advertisement multiple times during the 2024 Super Bowl that featured a young-looking animated cartoon protagonist in an animated cartoon world who uses magic to bestow low-priced Temu products on everyone she encounters. (See Figure 3) Attorneys General from several states as well as members of Congress urged CBS not to run the ad given ongoing investigations by Congress into Temu, and the company's documented relationship with the Chinese Communist Party. As one congresswoman who objected to the advertisement observed, it "looked like it belonged on a children's show."[64]

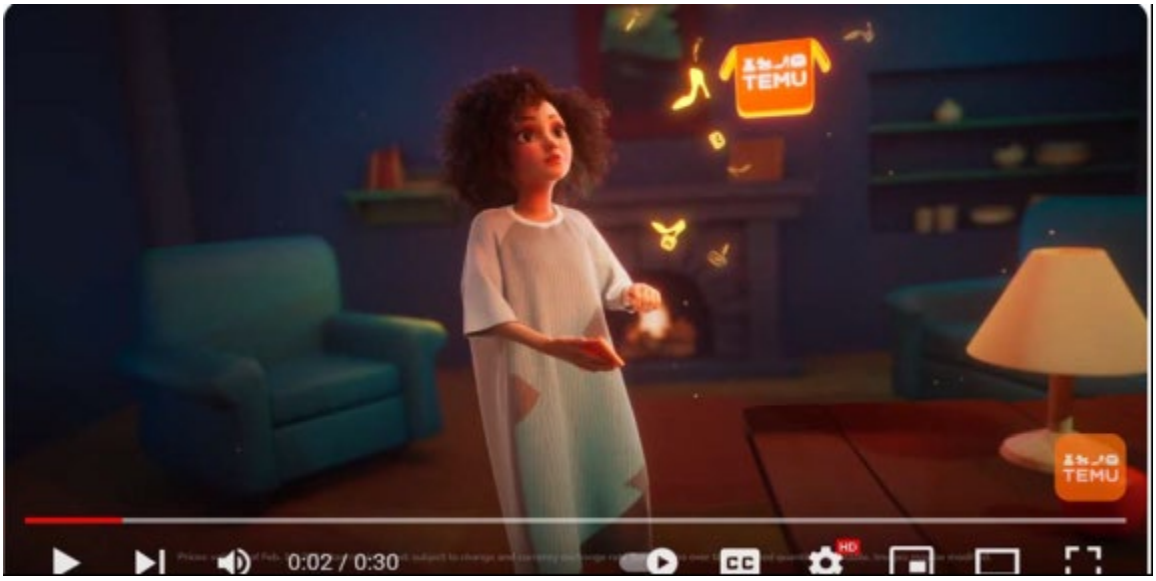

Figure 3: Screen capture of Temu's 2024 Super Bowl commercial.

[63] 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.

[64] *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.

178. Thus, notwithstanding Temu's statement in its terms of service that "[children] under 13 years are not permitted to use Temu or the Services,"[65] 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.

179. Temu's data collection procedures with respect to minors have also been a specific concern of government authorities. For example, in their ongoing investigation of Temu, members of Congress recently sent a letter to Defendants specifically requesting information regarding Temu's data collection practices with respect to minors.[66]

180. 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.

E. Temu Subjects User Data to Misappropriation by Chinese Authorities

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

182. Chinese law requires Chinese citizens, and individuals and entities in China to cooperate with national intelligence work undertaken by the Chinese government, and grants

[65] *Terms of Use*, Temu (Nov. 7, 2025), https://www.temu.com/cz-en/terms-of-use.html.
[66] *See* Letter from Cathy McMorris Rogers & Gus M. Bilirakis to Qin Sun, *supra* note 10, at 3.

regulators broad authority to access private networks, communication systems, and facilities to conduct invasive inspections and reviews.

183. 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.

184. 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."[67]

185. 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."[68]

---

[67] Tanner, *supra* note 8 (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.

[68] 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).

186. 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."[69]

187. 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. . . ."[70]

188. 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."[71]

189. 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."[72]

190. 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 . . . ."[73]

191. 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]

---

[69] 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/.
[70] *Id.* art. 7.
[71] *Id.* art. 14.
[72] *Id.* art. 16.
[73] *Id.* art. 17.

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."[74]

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

193. "China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime."[75]

194. 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."[76]

195. 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."[77]

---

[74] Zheng, *supra* note 67.
[75] 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.
[76] *Id.*
[77] 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.

196. 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."[78]

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

198. For example, Article 35 provides that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council."[79]

199. 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.[80]

200. Since the law's enactment, authorities have issued regulations expanding its scope.[81]

---

[78] *Id.* art. 49.
[79] *Id.* art. 35.
[80] *Id.* art. 37.
[81] *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.

201. 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.[82]

202. 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,"[83] 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.[84] 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.[85] CAC eventually imposed a $1.2 billion fine on the company.[86]

---

[82] *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 82; Gong, *supra* note 82. *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).

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

[84] *Id.*; Li, *supra* note 82.

[85] Horsley, *supra* note 83.

[86] *Id.*

203. 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."[87]

204. 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."[88]

205. 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[.]"[89]

206. 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."[90] 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."[91]

---

[87] 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.
[88] *Id.* art. 24.
[89] *Id.* art. 31.
[90] Haldane, *supra* note 67.
[91] 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.

207. 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.[92]

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

209. 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.

---

[92] *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, https://www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html (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 & 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).

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

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

211. None of the above is speculation or hyperbole. In a filing to the SEC on April 28, 2025,[93] Pinduoduo (1) acknowledges that Temu is one of its platforms,[94] 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."[95]

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."[96]

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."[97]

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

[93] PDD Holdings, Form 20-F Annual Report (2024), *supra* note 13.
[94] *Id.* at 1 (disclosing that "references in this annual report to [. . .] 'our platforms' are to the Pinduoduo platform and the Temu platform").
[95] *Id.* at 11, 51.
[96] *Id.* at 51.
[97] *Id.* at 52.

Laws') impose cybersecurity review obligations on [. . .] network platform operators that hold the data of more than one million users[.]"[98]

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."[99]

212. In sum, Temu exfiltrates Iowans' PII without their knowledge or consent, and has been designed to purposefully *hide* this harmful conduct. This privacy injury is compounded by the fact that the exfiltrated data also risks being appropriated by the Chinese government—a fact Iowans are never apprised of.

VI. TEMU's COMMERCIAL HARMS

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

213. "Disorganized, Discombobulated, and Unhelpful," is how one Iowa consumer describes their experience with Temu. Another Iowa consumer describes Temu as "terrible and deceitful." Defendants actively utilize deceptive and unfair practices in order to maximize the number of users who sign up to use the app, thereby maximizing the amount of data that Defendants can misappropriate. According to one commentator, "TEMU is a notoriously bad actor in its industry. We see rampant user manipulation, chain-letter-like affinity scams to drive signups,

[98] *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).

[99] PDD Holdings, Form 20-F Annual Report (2024), *supra* note 13, at 8.

and overall, the most aggressive and questionable techniques to manipulate large numbers of people to install the app."[100]

214. 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.

215. These gimmicks have been wildly successful: "PDD's TEMU online marketplace is being reported as among the fastest uptaken apps in history."[101]

216. 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,"[102] there have been

[100] *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/.

[101] *Id.*

[102] *About Temu*, Temu, https://www.temu.com/about-temu.html (last visited June 23, 2026).

numerous complaints regarding the quality of goods sold on the site as well as the service provided by Temu.

217. Temu customers in Iowa have submitted dozens of complaints to the BBB and Iowa Attorney General about Temu over the past three years. The experiences of consumers recounted below are merely concrete (but by no means exhaustive) examples of the countless acts by Temu that constitute violations of the Iowa Consumer Fraud Act. One thing, however, is clear: Iowa consumers feel that Temu has deceived them.

218. As demonstrated in numerous Iowa Better Bureau Complaints, Temu's "customer service" merely uses cut and paste canned responses when responding to consumer complaints, rarely actually responding to the issue at hand. Multiple Iowa consumers complained to the Better Business Bureau that even after returning goods to Temu, they never received a refund. And many others complained of receiving goods they never ordered, some of which they were charged for and unable to receive refunds for.

1. Deceptive Representations as to the Quality of Goods

219. The Better Business Bureau alone has received nearly 2,000 complaints nationally in the past year, earning Temu a rating of 2.1 out of 5 stars.[103] 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.

220. For example, one analysis observed that "TEMU products as shipped often do not resemble the photos."[104] Users frequently receive low-quality, cheaply-made merchandise when

[103] 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/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf.
[104] Grizzly Research, *supra* note 100.

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.[105] In addition, while Defendants claim that they use "world-class manufacturers" and have "strict policies against counterfeit or unsafe goods,"[106] 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).[107] Additionally, in November 2024, an Iowa consumer ordered a mattress from Temu. After about 16 months, the mattress started to severely sag.

2. Pricing Misrepresentations

221. 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.

222. Defendants engage in such false reference pricing on Temu. Examples of false reference pricing can be seen in Figures 6 through 12 in Paragraph 247, *infra*. Among the

[105] 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.

[106] *Temu's Commitments*, Temu, https://www.temu.com/commitments.html (last visited June 23, 2026).

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

ubiquitous misrepresentations about discounts and price representations in those images are statements that an item is offered for "the lowest price ever," "Lowest Price in 30 Days," "68% off," and progress bars and statements falsely representing that the item is part of a "Big Sale" that is nearly over and that price will increase in a short time unless the consumer purchases the item immediately. These are merely examples of the myriad ways in which nearly every Temu item listing includes representations designed to mislead consumers into believing that the item is offered at a significant discount from actual price for the item, that the price will only be available for a limited time, and/or there are limited quantities of the item available which will be gone if the consumer does not make an immediate purchase.

3. Charges for Goods Not Ordered or Not Delivered

223. Numerous Iowa 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.

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

225. **In January 2023**, an Iowa consumer called Temu "Disorganized, Discombobulated, and Unhelpful." The consumer "[r]eceived a package in the mail for [a] product [they] didn't order" with a return address to a person, rather than a company. When the consumer attempted to call Temu's customer service, the Temu representative could not find an order or tracking number, and continually asked for the customer's personal information.

226. **In May 2023**, an Iowa consumer ordered $63.00 of merchandise from Temu that never shipped. Temu refused too issue a full refund, merely offering the consumer $10.00 in credit.

227. **In August 2023**, an Iowa consumer received an order from Temu with a missing item. Temu refused to issue the consumer a refund.

228. **In November 2025**, an Iowa consumer received an email from Temu saying their mattress was on the way, despite never ordering a mattress. The consumer attempted to contact Temu before it arrived, but was unable to reach them and the mattress was delivered. The consumer then realized that they had an overdraft in their account because of Temu. The consumer had previously ordered Christmas decorations from Temu. After the mattress situation, the consumer continued to receive items they never ordered from Temu.

229. **In December 2025,** an Iowa consumer received incorrect items shipped by Temu. When they attempted to resolve the issue, they were told to cancel their order to receive a refund, but they never received their refund.

4. Sign-Up Scams, Gamification, Store Credit, and Failure to Honor Terms

230. Defendants utilize additional deceptive marketing techniques by presenting consumers with games, promotions, and other promises of rewards in exchange for users fulfilling requirements like: carrying out actions on the Temu app; placing a certain number or value of items in the consumer's "shopping cart"; purchasing products of a particular type, a certain number of products or total value of products; making purchases within a certain time frame; providing personal information about themselves and their friends and acquaintances; successfully getting other customers to sign up for and/or make purchases through the App; and/or spending a certain amount of time on the App. 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. Defendants promise users that when the user performs the stated terms of the games or promotions, Defendants will reward the user with incentives including free shipping on orders, free items, free items under a certain price, or store credit to put toward buying other items on Temu.

231. However, Defendants systematically fail to deliver on their statements to consumers about the terms of games and promotions. For example, after a consumer fulfills the stated requirements to earn a reward, Defendants notify the consumer about new, previously undisclosed requirements before the reward will be given; a promise of six free items if a user makes a purchase of at least $20 suddenly requires the user to forward an invitation sign-up link to a certain number of friends; Defendants' promise of a free item if a user merely places five items in their shopping cart suddenly requires the user to complete the purchase of those items before the free item can be earned. Other times, Defendants never deliver the promised rewards at all, even after a user completes all the required actions; a user who is promised "free shipping" on an order as a game reward is informed they must first pay for shipping and then apply to Defendants for reimbursement, which Defendants refuse to pay.

232. In addition, Defendants' offers of store credit and free items to users who get their friends and acquaintances to sign up for the app, often come with the hidden consequence that "[t]hose who do register are subjected to a bombardment of emails and app notifications."[108] "[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

[108] James Titcomb, *Here comes Temu, China's 'scary' bargain-basement Amazon killer*, The Telegraph (July 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/.

users fall down this rabbit hole, TEMU sends a torrent of popup sequences milking users for 'just one more contact'."[109]

233. Temu users are also bombarded by notifications and spam from third parties other than Defendants. These emails and notifications occur even after users opt-out of all communications from Temu.

234. Numerous Iowa Consumers have experienced these deceptions first-hand. For example:

235. **In September 2023**, an Iowa consumer received spam texts from Temu, despite never signing up for them, let alone visiting Temu's website, downloading the Temu app, or shopping with them.

236. **In October 2023**, an Iowa consumer made numerous referrals that they were never paid for.

237. **In November 2023**, an Iowa consumer claimed that "Temu is falsely advertising $750.00 credits for people to 'spam' other users."

238. **In March 2024**, an Iowa Consumer placed an order on Temu "because the statement on the app was spend up to 50 dollars get up to 50 back. [The customer] assumed this would be in credit." However, the customer received "coupons of 10 off of 100," which made the consumer feel completely deceived and caused them to cancel the order altogether. However, the order still shipped, and Temu refused to cancel the order or refund the consumer. The consumer said, "This company is terrible and deceitful."

239. **In April 2024**, an Iowa consumer complained to the Better Bureau Business that Temu was using false advertising, claiming if you shared a link and invited three friends, you could

[109] Grizzly Research, *supra* note 100.

claim free gifts. The consumer never received their "free gifts." In the customer's words, "FALSE ADVERTISEMENTS THE FALSE STATEMENTS AND THE FALSE ACTIVITY COMPLETED RULES TO GET FREE GIFTS. IT'S ALL A LIE"

240. **In August 2024**, an Iowa resident was deceived by Temu after they saw an ad stating they would receive a $300 credit if they purchased so many items. However, when they went to check out, the consumer was billed a different amount than the listed price of the item and never received their $300 credit.

241. **In November 2024**, an Iowa consumer played one of the games on Temu and won a $30 coupon. The consumer never received the coupon, but instead received "a random item worth $2.97."

242. **In January 2025**, an Iowa consumer placed an order on Temu after seeing an advertisement which said, "Place an order of $15 or more and receive three free gifts." The consumer selected their three gifts and paid for their order. However, the gifts disappeared from their order. When the consumer tried to cancel their order, they were told they could only receive credit to Temu.

243. **In March 2025**, an Iowa consumer played the "farmland" game on Temu, which promised them if they won, they would receive rewards. However, the consumer never received the promised awards. The consumer claims they have "spent hundreds of dollars on items to further [their] progression in game" but never received what they were promised.

244. **In April 2025**, an Iowa consumer never received the referral bonus they were promised. When they complained to Temu, they were offered a $10 credit. but it never appeared in their account.

245. **In June 2025**, an Iowa consumer got an alert on their phone from Temu that they had received free gifts. When they logged in and "spun the wheel," they were told they received over $350 "of free stuff" but they had to order a certain number of items to collect their reward. The consumer felt like Temu deceived them, because their receipt was for $117, but they ended up being charged even more than that.

246. **In July 2025**, an Iowa consumer downloaded the Temu app, and spun a prize wheel for discounts, winning three items for a penny each. The customer never received these items, despite paying for other items in order to claim these prizes. When they complained to Temu, they were told they had only completed 99.68% of the game, coming up short to win the items, despite spending over $700 to receive the bonus and receiving an alert saying "Congrats you made it" after winning the game.

247. **In April 2026**, an Iowa consumer wrote to the Better Business Bureau, "[t]he promos are scams . . [.] I've never gotten any of my free items."

5. Fake Reviews

248. Defendants attract and maintain users through other fraudulent means. For example, "TEMU [. . .] compensates users to write reviews," which are then "obviously skewed positive[.]"[110] 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

[110] *Id.*

person gave the item 5 stars which is impossible."[111] 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."[112] 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.

6. Intellectual Property Theft

249. Temu claims to be "committed to protecting everyone's intellectual property and [to] have a comprehensive policy to that end."[113] 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.[114]

250. 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 except for locating each listing separately and providing Temu with each specific listing URL link

---

[111] *Id.*

[112] 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/.

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

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

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.[115]

251. As a result of Temu's convoluted and ineffective IP protection policy, the Temu store is rife with unlicensed products listed for sale bearing protected trademark images. Countless brands are impersonated on the store, including the University of Iowa (and the IOWA Wave), Art's Way, and Dowling Catholic. (See Figures 5–11).

Figure 5: Temu product listing for counterfeit University of Iowa Basketball merchandise.

[115] *How to Take Down Counterfeit Listings on Temu*, IP Moat, https://ipmoat.ai/blogs/how-to-guides/how-to-remove-copied-product-listings-from-temu (last visited June 23, 2025).

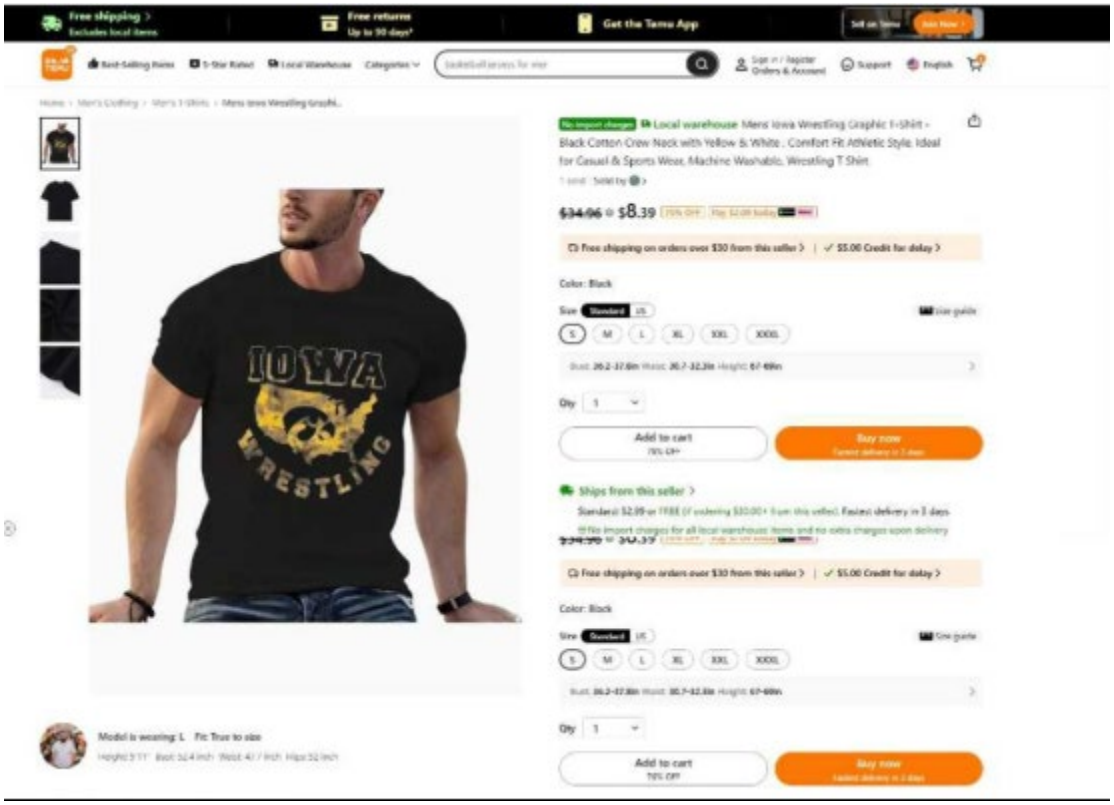

Figure 6: Temu product listing for counterfeit University of Iowa Wrestling t-shirt.

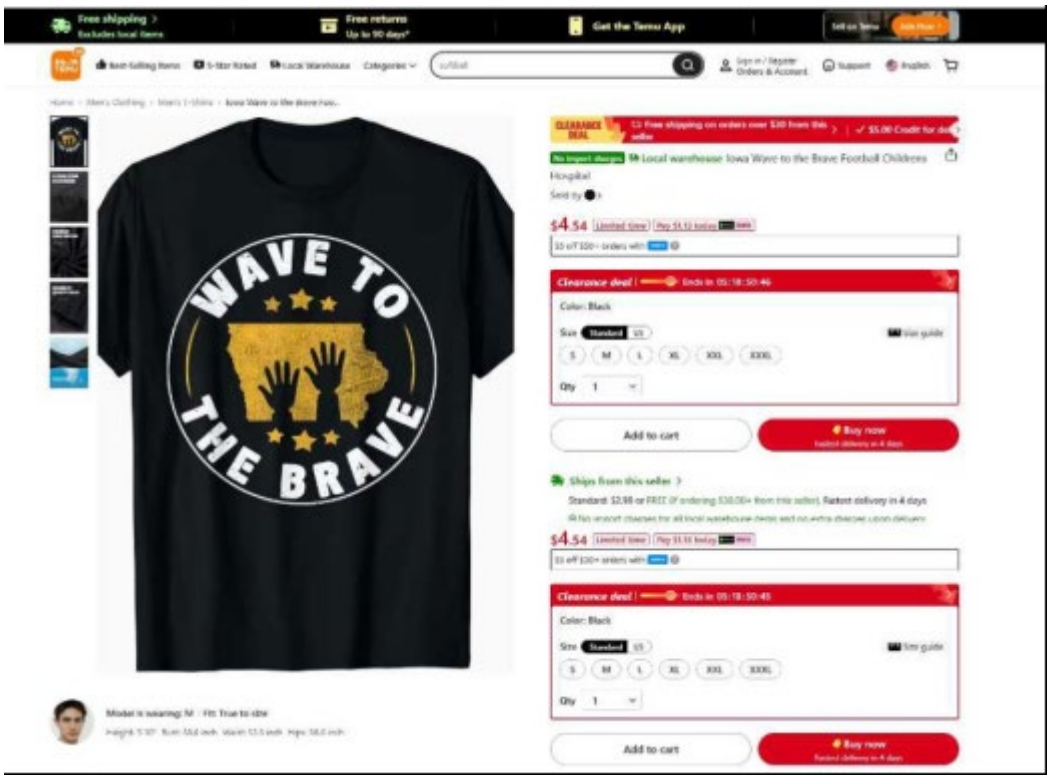

Figure 7: Temu product listing for counterfeit University of Iowa, Iowa Wave t-shirt.

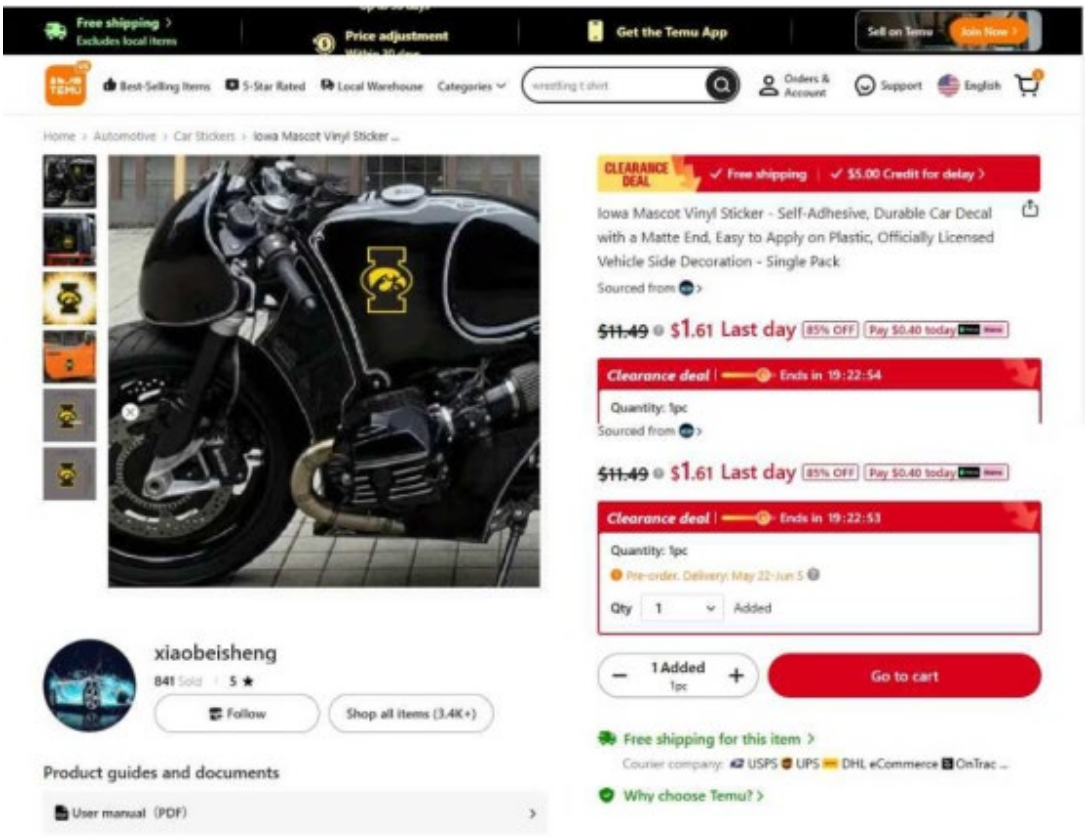

Figure 8: Temu product listing for counterfeit University of Iowa merchandise.

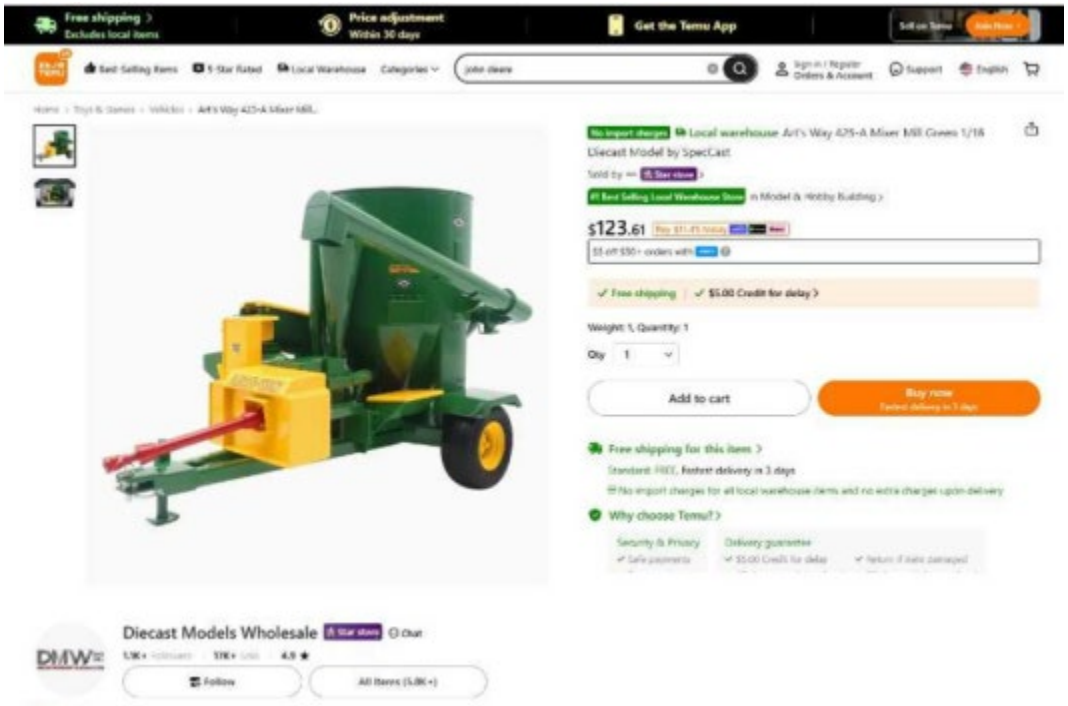

Figure 9: Temu product listing for counterfeit Art's Way merchandise.

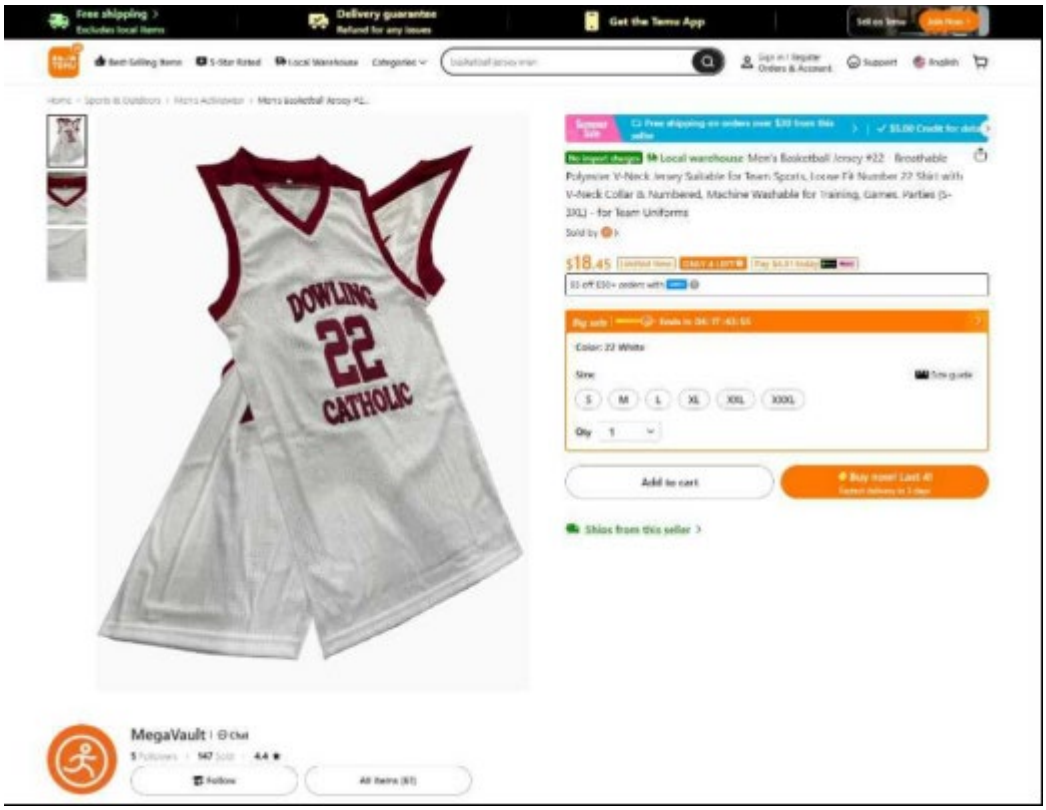

Figure 10: Temu product listing for a counterfeit Dowling Catholic basketball jersey.

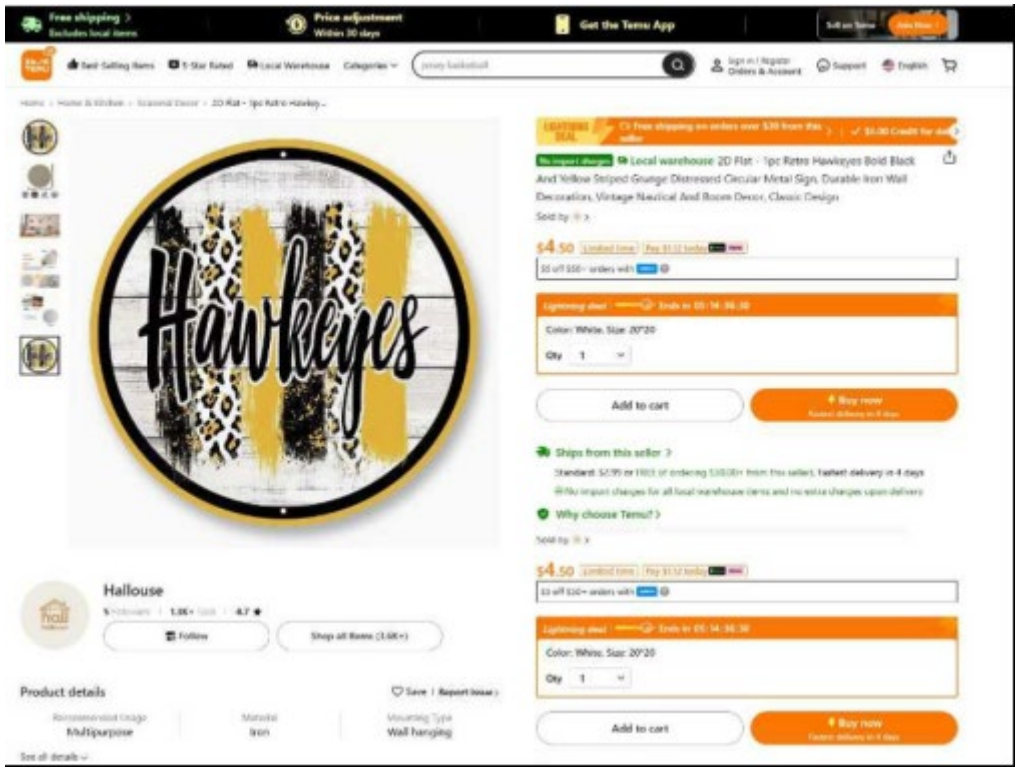

Figure 11: Temu product listing for a counterfeit "University of Iowa" merchandise.

252. It's pretty disturbing that one of the counterfeit goods serves as a replacement for the official goods related to the Iowa Wave, where proceeds for the official goods benefits the Iowa Stead Family Children's Hospital ("UISFCH") by supporting "enhanced care, new and innovative research at UISFCH through the Iowa Wave Shirt Pediatric Research Fund, the Adolescent and Young Adult Cancer Center and care within the Child Life Program."[116]

253. Furthermore, multiple Iowans have issued complaints to the Better Business Bureau that they have found images of products they sell on other websites, utilized on Temu to sell goods that are not theirs. A sampling of these complaints includes:

- **In November 2023**, an Iowa consumer claimed that Temu used their copyrighted images and videos without the consumer's permission;
- **In December 2023**, an Iowa consumer alleged that Temu stole their company's images;
- **In July 2024** an Iowa consumer reported that Temu used their images without authorization. The resident sells products on Amazon, and claimed that Temu used the images from Amazon to sell products on its own website;
- **In November 2024**, an Iowa resident reported that Temu was using their BARKLESS Brand Product images without authorization. The resident, an Amazon seller and owner of the BARKLESS brand, claims that Temu stole images of their inflatable dog cones to market products on its platform.

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

[116] *About the Iowa Shirt Wave*, Iowa City Wave, https://theiowawaveshirt.org/about (last accessed June 24, 2026).

7. Use of Forced Labor

255. In addition, while Defendants claim that they seek to "[d]o good for the world," are "honest, ethical and trustworthy," and are "socially responsible,"[117] 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.[118] 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."[119]

256. As the article explains, "Citing what the U.S. State Department has called 'horrific abuses' against the Uyghur people of Xinjiang, who are predominantly Muslim, federal officials banned the importation of cotton from the region in 2021 and expanded the law and its enforcement to all Xinjiang products last year under the Uyghur Forced Labor Prevention Act. Statements from former detainees and reports from an array of researchers and advocacy groups have alleged that the Chinese government put more than 1 million people in detention camps in the region and that laborers in fields and factories were forced or coerced."[120]

257. 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,

---

[117] *About Temu*, *supra* note 102.
[118] 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.
[119] *Id.*
[120] *Id.*

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.[121] 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.[122]

258. 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."[123] The report concluded that Temu is actively seeking to avoid the protections in place to prevent the sale of goods manufactured with forced labor: "Temu's business model … is to avoid bearing responsibility for compliance with the UFLPA and other prohibitions on forced labor while relying on tens of thousands of Chinese suppliers to ship goods direct to U.S. consumers."[124] Moreover, the report observed that "Temu admitted that it 'does not expressly

[121] Kaufman, *supra* note 103.
[122] 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),https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-krishnamoorthi-send-letters-forced-labor-concerns-nike-adidas-shein.
[123] Staff of H.R. Select Comm. on the CCP, *supra* note 33, at 2.
[124] *Id.*

prohibit third-party sellers from selling products based on their origin in the Xinjiang Autonomous Region.'"[125]

259. 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."[126]

260. 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[.]"[127] 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."[128]

261. 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.

8. "Greenwashing"

262. 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

[125] *Id.*
[126] *Id.* at 3.
[127] *Id.* at 7.
[128] *Id.* at 9.

"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.

263. Beginning in at least July 2023, Temu claims that it has planted more than 24 million, through a charity called "Trees for the Future," without disclosing any information about what portion of each sale is donated to charity. Temu has made claims to consumers that donations to Trees for the Future are "funded by users worldwide who donate by clicking 'Donate to Trees for the Future' at checkout. *Temu also separately contributes to this initiative*."[129] (Emphasis added). Trees for the Future displays its "Corporate Partners" on its website, ranking them by the "number of trees planted" by each partner.[130] The charity lists thirty "Corporate Partners" that have "planted" more than 1-million trees. Temu is listed as one of the two largest "tree planters," with 25 million trees funded. 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.[131]

264. 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.

---

[129] *Temu's Tree Planting Program*, Temu, https://www.temu.com/tree-landing.html (last visited June 23, 2025).
[130] *There's Power in Partnership*, Trees for the Future, https://trees.org/corporate-sponsorships/ (last visited June 23, 2026).
[131] *Financial Statements for the Year Ended December 31, 2023* at 5, Trees for the Future (Nov. 15, 2024), https://trees.org/wp-content/uploads/2024/11/TREES-2023-Audit-Report.pdf.

VII. CAUSES OF ACTION

A. Claims Under the Consumer Fraud Act and Civil Penalties

265. Under the Iowa Consumer Fraud Act:

> The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice.

Iowa Code § 714.16(2)(a).

266. Defendants have engaged and continue to engage in the sale and advertisement of merchandise as defined in the Act, with hundreds of thousands of Iowans. Merchandise "includes any objects, wares, goods, commodities, intangibles, securities, bonds, debentures, stocks, real estate or services." *Id.* § 714.16(1)(e).

267. Defendants sell actual objects, wares, and goods.

1. Privacy Harms

268. The conduct described in the preceding paragraphs of this Petition constitutes "unfair practice, deception" and "misrepresentation" in violation of the Act. *Id.* § 714.16(2)(a).

269. As described *supra* in Sections I through VI, and under the guise of offering cheap products to Iowa consumers, Temu secretly collects vast amounts of sensitive user data—including location, contacts, audio, camera, device identifiers, and app activity—while employing sophisticated evasion tactics such as code obfuscation, encrypted transmissions, root detection, and unauthorized system access designed to prevent both users and security researchers from discovering the types and extent of data being collected. Temu users are not given meaningful notice or control over this data collection.

270. The unfair, false, misleading, and/or deceptive acts committed by Defendants to secretly collect sensitive user data constitute unlawful conduct under the CFA and have caused or are likely to cause substantial injury to Iowa consumers.

271. Without an injunction from this Court, Temu is likely to continue these practices, which would further harm both consumers and cause harm to the public.

272. Each instance of Defendants' unfair and deceptive practices constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

2. Commercial Harms

273. Additionally, Temu has made false, misleading, and/or deceptive representations about the products they sell to Iowa consumers. As described in Section VI above, Defendants engaged in unfair and deceptive acts and practices in the marketing and sale of goods to Iowa consumers. These unfair and deceptive acts and practices include:

a. Misrepresenting the characteristics and quality of goods offered for sale and advertising products for sale that bear no resemblance to the pictures and descriptions of the products advertised;

b. Misrepresenting to consumers that countless products are, for a limited time or quantity, offered at steeply discounted prices below the stated "real price," when in fact those products are never offered for sale at a price anywhere near the "real price" that Temu claims;

c. Charging consumers for goods and products that are never delivered to the consumer, or which the consumer never even ordered, and delivering mysterious and unexpected packages to consumers that they did not order;

d. Misrepresenting to consumers that Temu is "honest, ethical and trustworthy," and "socially responsible," while failing to disclose to consumers that numerous products are manufactured using forced labor in foreign countries;

e. Engaging in misleading and deceptive marketing techniques to induce existing users to recruit other users and then spamming to sign up for the Temu platform;

f. Posing false and misleading reviews of products to entice consumers to purchase products based on those reviews;

g. Using games and promotions to entice users to make purchases or to sign up new users, and then failing to provide the reward incentives promised to users in its games and promotions;

h. Offering countless products for sale to consumers that are falsely represented to be authentic and/or licensed by intellectual property rightsholders when those products are not actually authentic products;

i. Falsely representing to consumers that Temu will donate a portion of the sale of its products to a charitable organization to plant trees, when in reality any donations made to the charity are either a de minimis amount of the sales price or else an extra charge to the consumer above the amount charged for merchandise.

274. The unfair, false, misleading, and/or deceptive acts committed by Defendants caused or are likely to cause substantial injury to Iowa consumers. Without an injunction from this Court, Temu is likely to continue these practices, which would further harm both consumers and cause harm to the public.

275. Each instance of Defendants' unfair and deceptive practices constitutes a separate violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7).

3. Reimbursement and Disgorgement

276. Through Defendants' deceptions, misrepresentations, false promises, and other unfair practices, Defendants have acquired moneys or property by a means unlawful under the CFA.

277. The CFA authorizes the court to "restore to any person in interest any moneys or property, real or personal, which have been acquired by means of a practice declared to be unlawful by this section[.]" Iowa Code § 714.16(7).

278. Further, where "the cost of administering reimbursement outweighs the benefit to consumers . . . the court may order disgorgement of moneys or property acquired by the person by the person awarding the moneys or property to the state to be used by the attorney general for the administration and implementation of" the CFA. Id.

279. For merchandise purchased by Iowa consumers related to Defendants' unlawful conduct" where the cost of reimbursement does not outweigh the benefit to consumers, the Court should order full reimbursement to Iowa consumers.

280. For all revenues gained by Defendants as a result of Defendants unlawful conduct where the cost of reimbursement outweighs the benefit to consumers, including circumstances where disaggregation of revenues to individual consumers will be difficult (e.g., revenue tied to privacy and security violations that are hard to attribute to individual consumers), the Court should order disgorgement of all of those revenues under Iowa Code § 714.16(7).

VIII. PRAYER FOR RELIEF

WHEREFORE, the State of Iowa, *ex rel.* Attorney General Brenna Bird, respectfully requests that the Court render judgement in the State's favor and:

a. Declare that Defendants have engaged in misrepresentations, deceptions, false promises, and unfair practices against Iowa consumers in violation of the Iowa Consumer Fraud Act, Iowa Code § 714.16, *et seq.*;

b. Preliminarily and permanently enjoin Defendants from engaging in the deceptive and unfair acts described in this petition;

c. Award the State civil penalties of $40,000 per violation under Iowa Code § 714.16(7);

d. Order reimbursement to Iowa consumers where possible in accordance with Iowa Code § 714.16(7);

e. Order disgorgement of all funds and property acquired by Defendants from Iowa consumers through their continued misrepresentations, deceptions, false promises, and unfair practices and award the funds and property to the State to be used by the Attorney General under Iowa Code § 714.16(7);

d. Award the State its costs and fees under Iowa Code § 714.16(11), including expert-witness expenses; costs incurred in pursuing this action and investigation, including reasonable attorneys' fees; and prejudgment and post-judgment interest at the highest lawful rates;

e. Declare that each Defendant is jointly and severally liable for all penalties and money damages awarded; and

e. Grant all other relief to which the State may be entitled.

DATED this 1st day of July, 2026.

Respectfully submitted,

BRENNA BIRD
ATTORNEY GENERAL OF IOWA

/s/ Laura L. Mommsen
Laura L. Mommsen
Assistant Attorney General
Daniel Barnes
Deputy Attorney General for Consumer Protection
1305 E. Walnut St.

Des Moines, Iowa 50319
(515) 281-8757
laura.mommsen@ag.iowa.gov
daniel.barnes@ag.iowa.gov

Brian E. McMath, *pro hac pending*
Dori Persky Tesser, *pro hac pending*
Brian Moore, *pro hac pending*
NACHAWATI LAW GROUP
5489 Blair Road
Dallas, Texas 75231
Telephone: (214) 890-0711
bmcmath@ntrial.com
dtesser@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

Counsel for Plaintiff State of Iowa