**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF NEW YORK**

----------x

ERIC HU,
EDWIN ANTONIO SURIS
TIMOTHY SMITH
ROY NORMAN MORROW
MING HUI LIN
NANCY BATALAS
JAMES LAFATA
DANIEL DAVID KATTAN
TRACY EVETTE STARLING
CHRISTOPH B. OH
HECTOR ANDREW CORDERO
YO-YO CHEN
MANISHA REDDY NARAYAN
*on behalf of themselves and others similarly situated,*

Case No. 23-cv-06962

Plaintiffs,

v.

WHALECO, INC.
d/b/a Temu,

Defendant.

----------x

---

**NATIONWIDE CLASS ACTION FIRST AMENDED COMPLANT**
**JURY TRIAL DEMANDED**

---

Plaintiffs ERIC HU, EDWIN ANTONIO SURIS, TIMOTHY SMITH, DEMETRIUS ALEXANDER DRIVAS, ROY NORMAN MORROW, MING HUI LIN, JAMES LAFATA, DANIEL DAVID KATTAN, TRACY EVETTE STARLING, CHRISTOPH B. OH, HECTOR ANDREW CORDERO, NANCY BATALAS, YO-YO CHEN and MANISHA REDDY NARAYAN (Collectively "Plaintiffs" ), bring this Class Action Complaint against Defendant WHALECO, INC. d/b/a Temu ("Defendant" or "Temu"), on behalf of themselves and others

similarly situated, and complains and alleges upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys:

## I. NATURE OF THE ACTION

1. Plaintiffs bring the proposed class action against Defendant on behalf of all persons who downloaded Temu, an application (the "Temu App"), and used Temu's in-app website browser.

2. Defendant discloses in the information it collects about the individuals who uses their App:

> **Personal information we collect**[1]
>
> **Information you provide to us.** Personal information you may provide to us through the Service or otherwise includes:
>
> - **Contact data**, such as your first and last name, salutation, email address, billing and mailing addresses, and phone number.
> - **Demographic Information**, such as your city, state, country of residence, postal code, gender and age.
> - **Profile data**, such as the username and password that you may set to establish an online account on the Service, **date of birth, redemption code, biographical details, photograph, links to your profiles on social networks, interests, preferences, information about your participation in our contests, promotions, or surveys**, and any other information that you add to your account profile.
> - **Communications** that we exchange with you, including when you contact us through the Service, **social media, or otherwise**.
> - **Transactional data**, such as information relating to or needed to complete your orders on or through the Service, including order numbers and transaction history.
> - **Marketing data**, such as your preferences for receiving our marketing communications and details about your engagement with them.
> - **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. Metadata includes

[1] https://web.archive.org/web/20230309172053/https://www.temu.com/privacy-and-cookie-policy.html

information on how, when, where and by whom a piece of content was collected and how that content has been formatted or edited. Metadata also includes information that users can add or can have added to their content, such as keywords, geographical or location information, and other similar data.

- **Government-issued identification numbers**, such as **national identification number (e.g., Social Security Number, tax identification number, passport number), state or local identification number (e.g., driver's license or state ID number), and an image of the relevant identification card**.
- **Payment information** needed to **complete transactions, including payment card information or bank account number**.
- **Promotional information**, including information you share when you enter a competition, promotion or complete a survey. Please note that if you participate in a sweepstakes, contest or giveaway through the Service, we may ask you for your Contact Data to notify you if you win or not, to verify your identity and/or to send you prizes. In some situations, we may need additional information as a part of the entry process, such as a prize selection choice. These sweepstakes and contests are voluntary. We recommend that you read the rules and other relevant information for each sweepstakes and contest that you enter.
- **Other data** not specifically listed here, which we will use as described in this Privacy and Cookie Policy or as otherwise disclosed at the time of collection.

**Third-party sources.** We may combine personal information we receive from you with personal information we obtain from other sources, such as:

- **Sellers**, including businesses and individuals who sell products on Temu.
- **Public sources**, such as government agencies, public records, social media platforms, and other publicly available sources.
- **Data providers**, such as information services and data licensors that provide demographic and other information, as well as credit bureaus, which help us detect fraud and offer certain credit-based services. This data may include your credit history information.
- **Our affiliate partners**, such as our affiliate network provider and publishers, influencers, and promoters who participate in our paid affiliate programs.
- **Marketing partners** such as joint marketing partners and event co-sponsors.
- **Third-party services**, such as
    - Social media services, that you use to log into, or otherwise link to, your Service account. This data may include your username, profile picture and other information associated with your account on that third-party service that is made available to us based on your account settings on that service. Exactly what information we receive will depend on your privacy settings with the applicable platform.
    - Logistics service providers, who help us calibrate our fulfillment services. This data

may include your delivery address 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 your computer's or mobile device's operating system type and version, manufacturer and model, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique identifiers (including identifiers used for advertising purposes), language settings, mobile device carrier, radio/network information (e.g., Wi-Fi, LTE, 3G), and general location information such as city, state or geographic area.
- **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.
- **Location data** when you authorize the Temu mobile app to access your device's location.

**Cookies and similar technologies.** Some of the automatic collection described above is facilitated by the following technologies:

- **Cookies,** which are small text files that websites store on user devices and that allow web servers to record users' web browsing activities and remember their submissions, preferences, and login status as they navigate a site. Cookies used on our sites include both "session cookies" that are deleted when a session ends, "persistent cookies" that remain longer, "first party" cookies that we place and "third party" cookies that our third-party business partners and service providers place.
- **Local storage technologies,** like HTML5, that provide cookie-equivalent functionality but can store larger amounts of data on your device outside of your browser in connection with specific applications.
- **Web beacons,** also known as pixel tags or clear GIFs, which are used to demonstrate that a webpage or email address was accessed or opened, or that certain content was viewed or clicked.

**Data about others.** We may offer features that help users invite their friends or contacts to use the Service, and we may collect contact details about these invitees so we can deliver their invitations.

3. Thus Defendant stores massive amounts of personal identifying information on its servers and utilizes this information to maximize its profits through predictive marketing and other

marketing techniques.

4. Plaintiffs bring this proposed class action against Defendant for its failure to secure and safeguard its customers' personal data, including name, address, email address, phone number, financial information (credit card information) and biometrics data (fingerprinting), and failing to provide notice to its app users after being in notice of several complaints from its app users about their personal information being compromised and further failing to take any reasonable steps to avoid from hackers to continue to steal personal and financial data from Defendant and put Class members' personal and financial information at serious and ongoing risk (the "Data Breaches" or "Breaches").

5. The Breaches were caused and were continued to be enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. Defendant grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Breach.

6. The Breaches, as complained of and reported to the Better Business Bureau, include multiple reports of credit card information and bank information being sold or leaked after use of Temu App.

7. The hackers continue to use the information they obtained as a result of Defendant's inadequate security to exploit and injure Class members across the United States.

8. Altogether, in the first instant Defendant failed to uncover and disclose the extent of the Breach and notify its affected customers of the Breach in a timely manner. Defendant failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Breaches. Furthermore, by failing to provide adequate notice, Defendant prevented

Class members from protecting themselves from the Breaches.

9. Plaintiffs further bring this proposed class action against Defendant for wiretapping the electronic communications of visitors to its website, www.temu.com.

10. As described more fully below, the in-app browser inserts JavaScript code into the website visited by Temu users. The clear purpose of the JavaScript code inserted into these websites is to track every detail about Temu users' website activity.

11. Through the use of its in-app browser, Temu has secretly and invasively amassed massive amounts of extremely private information and data about its users by tracking their activity on third-party websites. Defendant has unlawfully intercepted private and personally identifiable data and content from Temu users so that Defendant may generate revenue from use of this data. Through their clandestine tracking activities, Defendant have violated wiretap laws, unlawfully intruded upon users' privacy, violated their rights of privacy, and unjustly profited from their unlawful activities.

12. What is more, unknown to its users, included in the Temu App is a software developed in China. The Temu App has clandestinely vacuumed up and transferred to servers in China (and to other servers accessible from within China) vast quantities of private and personally identifiable user data and content that could be employed to identify, profile, and track the physical and digital location and activities of United States users now and in the future.

13. Defendant and their sophisticated engineering teams also covertly collect and use Temu App users' highly sensitive and immutable biometric identifiers and information.

14. Defendant unjustly profit from the secret harvesting of this massive array of private and personally identifiable Temu App user data and content by using it for targeted advertising, improvements to the development of consumer demand for, and use of, Defendant' products.

15. Temu App accesses its users' data for various purposes, including tracking users by age, gender, location, operating system, and interest in order to attract marketing and ad sales.

16. Congress passed the Wiretap Act to protect the privacy of the people of the United States. The Wiretap Act is very clear in its prohibition against intentional unauthorized taping or interception of any wire, oral, or electronic communication. In addition to other relevant sections, the Wire Tap Act states that any person who: "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" has violated the act. 18 U.S.C. §2511.

17. Defendant' conduct violates statutory, constitutional, and common law privacy, data, biometrics and consumer protections, and it should be stopped.

18. Plaintiffs bring this action for every violation of the Wiretap Act which provides for statutory damages of the greater of $10,000 or $100 per day for each violation of 18 U.S.C. §2510 *et seq.* under 18 U.S.C. §2520.

19. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, asserts claim for breach of implied contract and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

## II. JURISDICTION & VENUE

20. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiffs claims and the claims of other members of the class exceed $5,000,000.00 exclusive of interest and costs, and there are numerous Class members who are citizens of States other than Defendant's State of citizenship.

21. This Court has personal jurisdiction over Defendant because Defendant continuously and permanently does business in New York and has established the requisite minimum contacts with New York.

22. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2), as a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

## III. PARTIES

### A. Plaintiffs

#### 1. New York Plaintiff ERIC HU

23. Eric Hu is a citizen of the State of New York. Hu downloaded the Temu App and purchased products on the platform, thereby subjecting Hu's personal and private data to misappropriation by Defendant.

#### 2. Florida Plaintiff EDWIN ANTONIO SURIS

24. Edwin Antonio Suris is a citizen of the State of Florida. Suris downloaded the Temu App and purchased the products on the platform, thereby subjecting Suris's personal and private data to misappropriation by Defendant.

#### 3. Illinois Plaintiff TIMOTHY SMITH

25. Timothy Smith is a citizen of the State of Illinois. Smith downloaded the Temu App and purchased the products on the platform. Despite downloading the Temu App and making purchases on the platform, he never received the orders he placed online. Instead, Smith experienced the misappropriation of his personal and private data by the Defendant. However, Smith never received the order he placed online rather, he was subjected to his personal and private data to misappropriation by Defendant.

#### 4. Massachusetts Plaintiff ROY NORMAN MORROW

26. Roy Norman Morrow is a citizen of the State of Massachusetts. Morrow downloaded the Temu App and purchased products on the platform, thereby subjecting Morrow's

personal and private data to misappropriation by Defendant.

5. **Pennsylvania Plaintiff MING HUI LIN**

27. Min Hui Lin is a citizen of the State of Pennsylvania. Lin downloaded the Temu App and purchased products on the platform, thereby subjecting Lin's personal and private data to misappropriation by Defendant.

**6. California Plaintiff NANCY BATALAS**

28. Nancy Batalas is a citizen of the State of California. Batalas downloaded the Temu App and purchased products on the platform, thereby subjecting Batalas's personal and private data to misappropriation by Defendant.

**7. Texas Plaintiff JAMES LAFATA**

29. James Lafata is a citizen of the State of Texas. Lafata downloaded the Temu App and purchased products on the platform, thereby subjecting Lafata's personal and private data to misappropriation by Defendant.

**8. Oregon Plaintiff DANIEL DAVID KATTAN**

30. Daniel David Kattan is a citizen of the State of Oregon. Kattan downloaded the Temu App and purchased products on the platform, thereby subjecting Kattan's personal and private data to misappropriation by Defendant.

**9. Georgia Plaintiff TRACY EVETTE STARLING**

31. Tracy Evette Starling is a citizen of the State of Georgia. Starling downloaded the Temu App and purchased products on the platform, thereby subjecting Starling's personal and private data to misappropriation by Defendant.

**10. New Jersey Plaintiff CHRISTOPH B. OH**

32. Christoph B. Oh is a citizen of the State of New Jersey. Batalas downloaded the

Temu App and purchased products on the platform, thereby subjecting Batalas's personal and private data to misappropriation by Defendant.

**11. Missouri Plaintiff HECTOR ANDREW CORDERO**

33. Nancy Batalas is a citizen of the State of California. Batalas downloaded the Temu App and purchased products on the platform, thereby subjecting Batalas's personal and private data to misappropriation by Defendant.

**12. Connecticut Plaintiff YO-YO CHEN**

34. Yo-Yo Chen is a citizen of the State of Connecticut. Chen downloaded the Temu App and purchased products on the platform, thereby subjecting Chen's personal and private data to misappropriation by Defendant.

**13. Washington Plaintiff MANISHA REDDY NARAYAN**

35. Manisha Reddy Narayan is a citizen of the State of Washington. Narayan downloaded the Temu App and purchased products on the platform, thereby subjecting Narayan's personal and private data to misappropriation by Defendant.

**B. Defendant WHALECO INC d/b/a Temu:**

36. Defendant WHALECO INC d/b/a Temu is a Delaware business corporation with its principal place of business in Massachusetts, doing business in all 50 States and the District of Columbia.

## IV. FACTUAL BACKGROUND

37. The speed of communications and rapidly changing consumer preferences and fashion have created strong consumer demand for the ultra-fast fashion business model. The unique characteristics of ultra-fashion requires market participants to act as e-commerce retailers, meaning all or virtually all of their sales come from online sales.

38. Temu entered the U.S. market in or around July 2022, becoming U.S. consumers'

favorite ultra-fast retailer, topping the app store charts and consistently offering lower prices than Shein, its major competitor in the field.

39. On December 24, 2022, during the peak of the holiday shopping season in the U.S., The Wall Street Journal, published an article dedicated to a retailer that had entered the market only three months prior. "American Bargain Hunters Flock to a New Online Platform Forged in China"[2] read the headline. The byline continued, "Temu, a marketplace with deep discounts and copious discounts, has become the most downloaded app in the U.S."[3]

40. The products offered on the Temu Platform include men's, women's, and children's apparel. Like Shein, nearly all Temu's product offerings in the U.S. come from a network of manufacturers located in China.

**A. A HERITAGE OF MALWARE**

41. After introducing the Pinduoduo app, Defendant through its parent company PDD Holdings Inc., went on to create a second online retail application called the "Temu" app. Many software engineers who played a key role in developing the Pinduoduo app were actively involved in crafting the "Temu" app. Notably, a significant aspect is that the majority of approximately 100 engineers, previously dedicated to developing the Pinduoduo app, which illicitly exploits collected user data without permission, were reassigned to contribute to the development of the Temu App[4]. Despite these ties, much

[2] https://www.wsj.com/articles/american-bargain-hunters-flock-to-a-new-online-platform-forged-in-china-11671851837
[3] I.d.
[4] https://nypost.com/2023/08/05/why-the-chinese-shopping-app-is-a-scam/; *see also*, https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html

like the approach taken by PDD Holdings, the Defendant have sought to mask Temu's connection to China (and the initial Pinduoduo app) by publicly asserting that "the Temu platform operates primarily in the United States."[5].

42. Analysts have found that Temu App, specifically, uses the allure of inexpensive Chinese-manufactured goods to entice users into unknowingly providing unwarranted and extensive access to their private data through deceptive methods.

43. Analysts went on to further assert that Temu's parent company Pinduoduo's data privacy policies and practices were deceptive, and many problematic features of the Pinduoduo app were shared with the Temu App. Reports indicated that Apple had also expressed similar concerns regarding the Temu App, stating that it did not comply with Apple's data privacy standards and that Temu was misleading users about how their data is utilized. As one report highlighted: "Apple said Temu previously violated the company's mandatory privacy rules. It found that Temu misled people about how it uses their data. Temu's so-called privacy nutrition labels, which describe 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."[6] Temu also isn't letting users choose not to be tracked on the internet.

44. Recently, government authorities have raised similar concerns after examining the app. For instance, the State of Montana has recently prohibited the use of the Temu App on government devices, along with other Chinese apps implicated in data privacy

[5] PDD Holdings Inc. Annual Report (2022).
[6] https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/

violations, such as Temu App[7]. This action, as explained by the State's Chief Information Officer when announced, aims to prohibit apps that present a risk of foreign adversaries obtaining Montanans' personal, private, sensitive information and data from government-issued devices.

45. Similarly, in April 2023, the U.S.-China Economic and Security Review Commission, a government entity established by Congress to investigate, assess, and report annually on the national security implications of the economic relationship between the United States and the People's Republic of China, released a report highlighting the significant data risks specifically associated with the Temu App[8].

46. Subsequent technical analysts have determined that the Temu App is deemed "even more 'malicious' than the suspended pinduoduo-6-49-0 app."[9] Analysts noted that Temu's data collection scope is extensive, surpassing what is necessary for the functioning of an online shopping app. According to one commentator, aside from Bluetooth and Wi-Fi access, "Temu gains full access to all your contacts, calendars, and photo albums, plus all your social media accounts, chats, and texts. In other words, literally everything on your phone.… No shopping app needs this much control, especially one tied to Communist China."[10] Another commentator, commenting on the Montana ban, expressed, "Temu is dangerous,' said tech writer Albert Khoury, warning

[7] https://www.theverge.com/2023/5/17/23727750/montana-bans-telegram-temu-wechat-other-bytedance-apps-government-devices-tiktok; *see also*, https://www.musicbusinessworldwide.com/montana-becomes-first-us-state-to-ban-tiktok/
[8] https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf
[9] https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shoppingapp-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/
[10] https://www.komando.com/kims-column/temu-security-concerns/883861/.

that the app 'bypasses' phone security systems to read a user's private messages, make changes to the phone's settings, and track notifications."[11]

47. Temu has been recognized as among the Chinese-affiliated applications posing a notable risk to user data privacy. Both experts in the field and government authorities have consistently highlighted the security risks linked to China-affiliated apps like TikTok and Temu App, emphasizing their infringement on users' data privacy rights in various manners. These observations have resulted in the imposition of restrictions on such Chinese apps and, in some cases, outright bans, driven by concerns regarding data privacy.

48. Through its marketing and advertisement, Defendant does not disclose and actively hide the existence of spyware on Temu users on its browser and cell phone applications.

49. According to a September 15, 2023 (last updated on September 21, 2023) CBS Chicago Investigation, entitled "Savings or Scam? BBB warns Temu takes personal info, citing hundreds of complaints," [12] by Dorothy Tucker, the consumer group Better Business Bureau has issued a warning about Temu. Specifically, Temu "collects all kinds of information, from your name, phone number, and address to your birthdate, social media photos, and social security number." "It also automatically collects data from your phone, tablet, or laptop information like the operating system, browsing history, and location data."[13]

---

[11] https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-governmentdevices-3694060; https://www.theverge.com/2023/5/17/23727750/montana-bans-telegram-temu-wechat-other-bytedance-apps-government-devices-tiktok

[12] https://www.cbsnews.com/chicago/news/bbb-temu-personal-info/

[13] I.d.

50. Like many other online vendors, Temu requires customers to disclose personal identifying information and processes customer credit and debit card payments.

51. Temu Application requests permissions including access to Bluetooth and Wi-Fi network information.

52. Temu Application draws on customer data and search history with the assistance of artificial intelligence algorithms to discern emerging fashion preferences and patterns.

53. To aid in its data collection, Defendant's app also requests that users share their data and activity from other apps, including social media.

54. The Better Business Bureau has amassed more than 900 complaints from consumers, including the unauthorized withdrawals from bank accounts and credit card purchases soon after the consumer began purchasing on Temu.

55. China's Cybersecurity Law, introduced in 2016 and enforced from 2017, obligates Critical Information Infrastructure operators to provide unobstructed access to their data to the government and mandates that such data be stored exclusively within mainland China.

56. Defendant's failure to comply with reasonable security standards provided Temu with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of its own customers—including Plaintiffs and the Class members here—who have been subject to the Breach or have otherwise had their personal identifying information placed at serious and ongoing risk.

***a. Website Users Have a Reasonable Expectation of Privacy in their Interactions with Websites***

57. Consumers are skeptical and are wary about their data being collected. A report

released by KPMG shows that "a full 86% of respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[14]

58. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website visitors will assume their detailed interactions with a website will only be used by the website and not shared with a party they know nothing about. As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[15]

59. Privacy polls and studies show that a majority of Americans believe that internet companies and website should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of data that has been collected about them.[16]

60. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected by them by companies.[17]

---

[14] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

[15] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[16] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[17] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019),

## B. IMPORTANCE OF DATA SECURITY TO PURCHASING DECISIONS

61. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiffs would not have made purchases at Temu, or would not have paid as much for them, had they known that Temu does not take all necessary precautions to secure their personal and financial data. Temu failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Temu.

62. Furthermore, when consumers make online purchases using Defendant's App, they enter into an implied contract with Defendant that Defendant will adequately secure and protect their Private Information, and will use part of the purchase price of the goods to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Temu simply kept the money to maximize its profits, thus breaching the implied contract.

63. Despite being in receipt of several app users' complaints against Temu pertaining to fraudulent charges and unauthorized use of their bank accounts or some of the emails accounts being compromised, Temu instead of taking adequate measures to stop it, rather allowed widespread and systematic theft of its customers' personal identifying information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' personal identifying information.

## C. VALUE OF PII TO COMPANIES AND HACKERS

---

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/

64. A Market exists for personal data and information regarding individuals' preferences and interests. This information is valuable because it can be compiled and sold as demographic data and advertising analytics or sold on a per-name basis. Companies like infoUSA compile consumer information and sell name and contact information categorized by demographic data, interests or other behavioral information.

65. It is well known and the subject of many media reports that PII data is also highly coveted by and a frequent target of hackers. PII data is often easily taken because it is less protected and regulated than PCD.

66. Thus, both legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "[o]ne of 2013's largest breaches . . . [n]ot only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users . . . ." [18]. Similarly, in the Target data breach in addition to PCD pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

67. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. Unfortunately, and as will be alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, Defendant's approach at maintaining the security of Plaintiffs' and Class Members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

## D. LACK OF SEGREGATION OF CARD HOLDER DATA FROM PII

[18] http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf

68. Unlike PII data, payment card data is heavily regulated. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

69. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data.

70. PCI DSS prohibits retailers such as Defendant from: (1) improperly storing and retaining credit card transaction and customer data in an unencrypted, unsecure, and unauthorized manner; (2) failing to render PCD on electronic media unrecoverable so that it cannot be reconstructed; (3) failing to properly install, implement and maintain firewall(s) to protect consumer data; (4) failing to properly limit inbound Internet traffic to certain IP addresses; (5) failing to perform dynamic packet filtering; (6) failing to properly restrict access to the business's computers; (7) failing to properly protect stored data; (8) failing to encrypt cardholder data and other sensitive information; (9) failing to properly use and regularly update anti-virus software or programs; (10) failing to track and monitor all access to network resources and cardholder data; and (11) failing to regularly test security systems or run vulnerability scans at least quarterly and after any significant network change.

71. One critical PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code.

72. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement." However,

segregation is recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after other personally identifiable information (PII) and corporate data."[19]

73. Many state statutes mandate additional data security requirements. For example, Cal. Civil Code § 1798.81 requires businesses to "take all reasonable steps to dispose, or arrange for the disposal, of customer records within [their] custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."

74. Illicitly obtained PII and PCD is sold on the black market, including on websites, as a product at a set price[20].

75. Without such detailed disclosure, Plaintiffs and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

## E. CONSEQUENCES OF DEFENDANT'S CONDUCT

76. According to the Plaintiffs and the Class members and including the review of the complaints filed with the BBB, the App User's data was breached when they registered their account with Temu and had provided their card information in the shopping app.

77. On information and belief, many of the app users reported that, their bank statements showed several unauthorized transactions following the use of Temu App.

[19] http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf
[20] *See e.g.*, https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/

78. On information and belief, Plaintiffs' Tracy Starlings, Nancy Batalas, James Lafata and Timothy Smith's identifying and/or financial information was compromised.

79. Plaintiffs Tracy Starlings, Nancy Batalas, James Lafata and Timothy Smith report that they never suffered any type of fraud, or identify theft before their data was breached.

80. Plaintiffs Tracy Starling and Nancy Batalas's experienced fraudulent activity in their bank account.

81. The following screenshot depicts the information provided to Plaintiff Tracy Starling concerning the fraudulent charges:

**IMAGE 1: Disputed Charge**

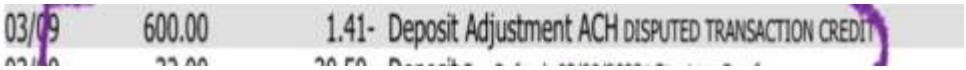



**IMAGE 2: Fraudulent Activities**


82. As a result, Plaintiff Tracy Starling was unable to use her bank accounts as a result of fraud.

83. On information and belief, the fraudulent charges on Plaintiff Starling's debit cards were traceable to Defendant's negligence and its failure to keep her personal and/or financial information secure.

84. Following Plaintiff James Lafata, registered his email address with Temu App and made purchases using the app. Plaintiff Lafata, experienced a series of unauthorized money deducted from his bank account from different portals such as cash app, Robinhood *etc*. Further Lafata's password was also changed for his email and bank accounts.

85. Plaintiff James Lafata, received notice from Microsoft Customer Support team stating that there is an unauthorized access to his Microsoft account. The hackers accessed Plaintiff Lafata's Microsoft account and further went on to change the security information for the account. Considering the change in the security information, and to further prevent the fraud, Microsoft Customers Support team had to permanently suspend his account.

**F. SECURITY BREACHES LEAD TO IDENTITY THEFT**

86. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying information ("PII") to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[21] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records… [and their] good name."

87. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve. Identity thieves use stolen PII for a variety of crimes, including

[21] *See* http:///www.gao.gov/new.items/d07737.pdf.

credit card fraud, phone or utilities fraud, and bank/finance fraud.[22]

88. A person whose PII has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

89. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[23] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other PII directly on various Internet websites, making the information publicly available, just as they have done here.

## G. THE MONETARY VALUE OF PRIVACY PROTECTION

90. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.

[22] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, alien registration number, government passport number, employer or taxpayer identification number." *Id*. (g)

[23] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009).

91. Though Commissioner Swindle's remarks are more than two decades old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[24]

92. The FTC has also recognized that consumer data is a new—and valuable—form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[25]

93. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share—and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.[26] This business has created a new market for the sale and purchase of this valuable data.[27]

94. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing

---

[24] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited February 10, 2023) ("Web's Hot New Commodity: Privacy").
[25] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited February 10, 2023).
[26] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited February 10, 2023).
[27] *See supra*, n.4.

to pay a premium to purchase from privacy protective websites."

95. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[28]

96. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII, like Temu, has deprived that consumer of the full monetary value of the consumer's transaction with the company.

## H. UNTHORIZED ACQUISITION OF PRIVATE AND PERSONALLY IDENTIFIABLE USER DATA AND CONTENT BY TEMU

### *a. Cache of Malware and Spyware in Temu App*

97. Unknown to Temu users is that the seemingly innocuous Temu App infiltrates their mobile devices and extracts a remarkably broad array of private and personally identifiable data and content that Defendant use to track and profile Temu users for the purpose of, among other things, targeting them with advertisements from which Defendant unjustly profits.

98. Plaintiffs, the Class, and the Subclass have a reasonable expectation of privacy in the private and personally identifiable data and content on their mobile device.

99. The United States Supreme Court has recognized that, in contemporary society, cell phones are so ubiquitous and inextricably intertwined with the user's personal privacy that such devices have become "***almost a 'feature of human anatomy***.'" *Carpenter v.*

[28] Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited February 10, 2023); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

*United States*, 138 S. Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). The United States Constitution thus provides a privacy right that protects individuals against unreasonable governmental searches of their physical movements through historical cell phone records in the possession of their service providers. *Carpenter*, 138 S. Ct. at 2218.

100. Temu App, operated by the defendant, collects a combination of user identifiers and mobile device identifiers from each mobile device on which it is installed. The information obtained includes various items, and the app's program code utilizes a range of functionalities to gain access to device resources.[29] Here's a brief overview of the mentioned terms:

a. *Location Code*: Used to get the user's precise location.

   i. android.permission.ACCESS_COARSE_LOCATION
   ii. android.permission.ACCESS_FINE_LOCATION

b. *Network and Connectivity Code*: Can be used to monitor the user's online activities:

   i. android.permission.ACCESS_NETWORK_STATE
   ii. android.permission.ACCESS_WIFI_STATE
   iii. android.permission.BLUETOOTH
   iv. android.permission.INTERNET

c. *Job Service Code*: Is used to allow the application to bind to a JobService, potentially impacting the user's device performance and raising concerns about unnecessary resource usage:

   i. android.permission.BIND_JOB_SERVICE

d. *Device Storage Code*: Reading and writing external storage can potentially grant access to user's sensitive data stored on the device.

29

i. android.permission.READ_EXTERNAL_STORAGE
ii. android.permission.WRITE_EXTERNAL_STORAGE

e. *System and Notifications Code*: RECEIVE_BOOT_COMPLETED code, is used to launch activities or services after the device boots up, potentially impacting the user experience and privacy.

i. android.permission.RECEIVE_BOOT_COMPLETED
ii. android.permission.POST_NOTIFICATIONS
iii. android.permission.WAKE_LOCK
iv. android.permission.VIBRATE

f. *Audio and Camera Code*: RECORD_AUDIO and CAMERA permissions can be exploited to capture audio or video without the user's consent, posing a significant privacy risk.

i. android.permission.RECORD_AUDIO
ii. android.permission.CAMERA

g. *Cloud Messaging and Authentication Code*: Codes related to cloud messaging and authentication may involve accessing and transmitting user data to third-party services, raising privacy concerns.

i. com.google.android.c2dm.permission.RECEIVE
ii. com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
iii. com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION
iv. com.google.android.gms.permission.AD_ID

h. *Badge Permissions Code (for specific device manufacturers)*: Badge permissions code for specific device manufacturers can be used to manipulate notification badges, potentially impacting the user experience. Reading and writing badge settings might also involve accessing user data.

i. com.huawei.android.launcher.permission.CHANGE_BADGE
ii. com.huawei.android.launcher.permission.READ_SETTINGS

iii. com.huawei.android.launcher.permission.WRITE_SETTINGS
iv. com.sec.android.provider.badge.permission.READ
v. com.sec.android.provider.badge.permission.WRITE
vi. com.vivo.notification.permission.BADGE_ICON

i. *Custom Permission Code*: The custom permission Code is used for remote configuration.

i. com.einnovation.temu.remote_config

***b. The Companion Note of All Available Updates of Temu App from Google Play Store Is Indeed More than a Generic "Bug Fixes and Improvements":***

101. All App permission changes that were made in the Temu App, since its launch was not a mere bug fixes and improvements. As more fully shown below, list of changes made to the app permission requests on Temu App Launch from 1.0.2 Version to 2.11.0, it can be seen how Temu has removed certain permissions from its App Permission requests such as:

i. **Removed**: Read Contacts & custom OEM perms; Removed BT & Alarm & Sensor & Sync perms; Removed A/M Account & c/f Location perms; Removed Record Audio perm; Removed Camera perm; Removed R/W External Storage perms; and Removed custom TEMU AB config perm[30].

j. **Added**: Added Read Contacts perm; Added High Sampling Rate Sensors perm; Added Adjust SDK Preloaded apps query perm; and Reinstated coarse/fine Location perms.

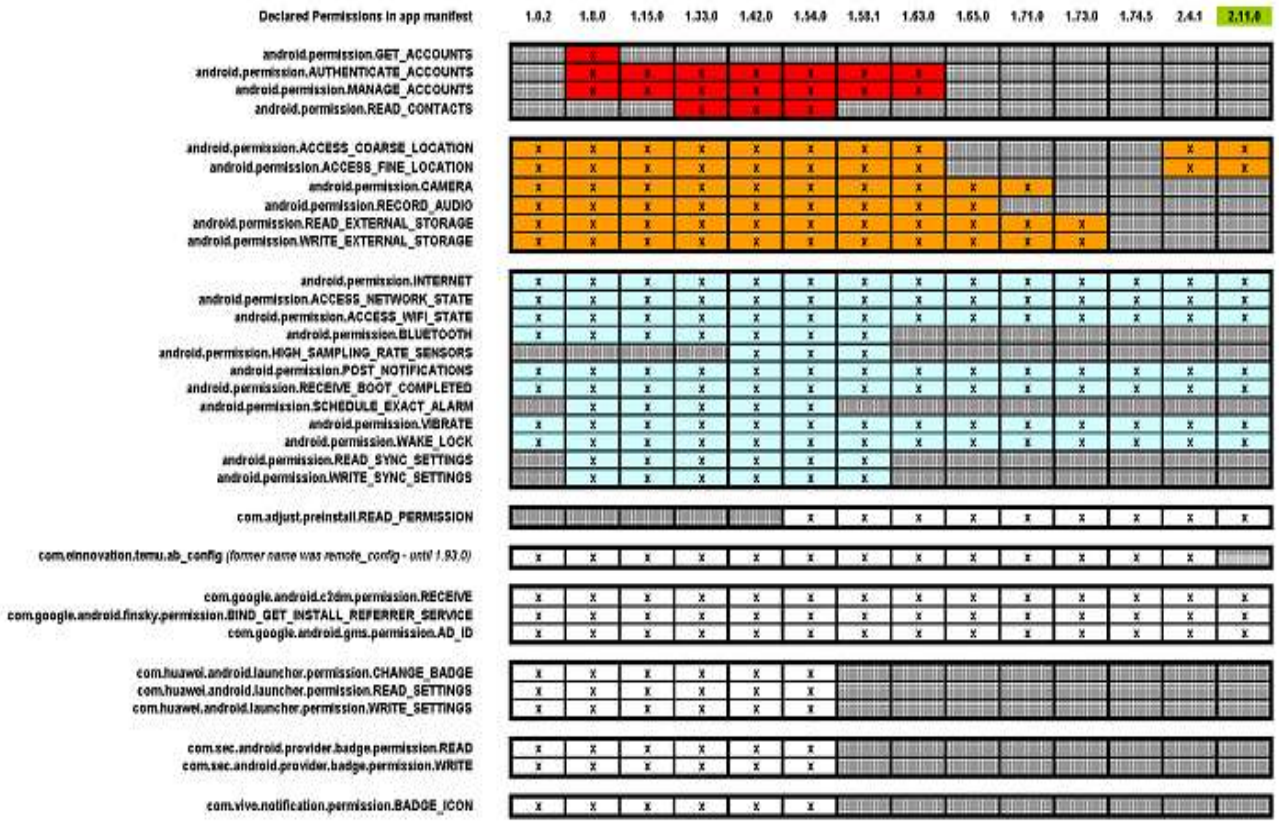
**Summary Table demonstrating all the Dates and Changes made to Temu App versions:[31]**

| Release Date | Version | Build | Perms | Notice |
|---|---|---|---|---|
| Aug 25, 2022 | 1.0.2 | 10002 | 24 | First Official release from Play Store |

[30] https://gitlab.com/rawmain/temu#53-obfuscation-manwe-wrapper-sdk
[31] https://gitlab.com/rawmain/temu#53-obfuscation-manwe-wrapper-sdk

| Release Date | Version | Build | Perms | Notice |
|---|---|---|---|---|
| Sep 29, 2022 | 1.8.0 | 10800 | 30 | Added R/W Sync + G/A/M Account + Alarm perms |
| Oct 27, 2022 | 1.15.0 | 11500 | 29 | First release using MANWE wrapper/SDK |
| Dec 30, 2022 | 1.33.0 | 13300 | 30 | Added Read Contacts perm |
| Jan 31, 2023 | 1.42.0 | 14200 | 31 | Added High Sampling Rate Sensors perm |
| Mar 15, 2023 | 1.54.0 | 15400 | 32 | Added Adjust SDK Preloaded apps query perm |
| Mar 20, 2023 | 1.55.2 | 15502 | 32 | Last release using MANWE wrapper/SDK |
| Apr 6, 2023 | 1.58.1 | 15801 | 24 | Removed Read Contacts & custom OEM perms |
| Apr 14, 2023 | 1.63.0 | 16300 | 20 | Removed BT & Alarm & Sensor & Sync perms |
| Apr 24, 2023 | 1.65.0 | 16500 | 16 | Removed A/M Account & c/f Location perms |
| May 18, 2023 | 1.71.0 | 17100 | 15 | Removed Record Audio perm |
| May 24, 2023 | 1.73.0 | 17300 | 14 | Removed Camera perm |
| May 31, 2023 | 1.74.5 | 17405 | 12 | Removed R/W External Storage perms |
| Sep 8, 2023 | 2.4.1 | 20401 | 14 | Reinstated coarse/fine Location perms |
| Oct 13, 2023 | 2.11.0 | 21100 | 13 | Removed custom TEMU AB config perm |
| **Nov 24, 2023** | **2.22.6** | **22206** | **13** | **Current latest release from Play Store** |

**Image Reflecting: Examining Declared Permissions in Temu App Manifest**



102. The Defendant's intrusive, covert, and illegal data gathering extends beyond the boundaries of the Temu App.

103. Defendant has accessed the clipboard on users' devices, allowing it to capture text and images that the user copied, even if in a different app, which could include passwords, financial information, or other sensitive, personally identifiable information.

104. The plaintiffs' scrutiny of the defendant's privacy policy brought to light that the defendant engaged in unauthorized data-mining and surveillance of user devices through automated technologies. The defendant, as explicitly stated on their website, admits to the automatic collection of user data through their affiliated partners. However, crucially, the defendant fails to disclose the comprehensive list of these affiliated partners, leaving users uninformed about the extent of data sharing. Furthermore, the defendant utilizes the automatically obtained information concerning the plaintiffs and other subclass members, including detailed insights into external websites visited beyond the application and the duration of time spent on those pages. This practice raises significant privacy concerns, as users are unaware of the breadth of data collection and its potential implications for their online activities. The lack of transparency regarding data sharing partners coupled with the extensive tracking of user behavior underscores the need for greater transparency and accountability in the defendant's data collection practices.

105. Simply put, Defendant did not obtain permission from users to access their devices, social media accounts, system clipboards, messaging apps, safari apps or other such

[32] *I.d.*

sensitive data and information.

***c. Temu App Covertly Stockpiles User Data and Device Information:***

106. Pinduoduo changed its corporate name to PDD Holdings Inc., which is now the parent company of both Pinduoduo App and Temu App[33].

107. Temu is owned by PDD Holdings, Inc., which is headquartered in China.

108. PDD Holdings Inc., established in 2015 by Chinese entrepreneur and software engineer Colin Huang, stands as a significant tech conglomerate in China. With a valuation surpassing $100 billion, it ranks among the country's largest companies. In the past years, the conglomerate recorded a gross operating profit exceeding $4 billion and a total revenue approaching $19 billion.

109. PDD Holdings Inc., with a network of subsidiaries in China, has traditionally housed its corporate headquarters in Shanghai. Despite this, there has been a recent disclosure indicating a shift in the "principal executive offices" to Dublin, Ireland, possibly as a move to obscure its ties to China. Nevertheless, the majority of PDD Holdings Inc.'s business operations, along with several subsidiaries, remain situated in China.

110. Engaged in diverse business endeavors, PDD Holdings Inc. operates Pinduoduo, an ecommerce platform established in China. This platform presents a wide array of products spanning categories such as agricultural produce, apparel, shoes, bags, mother and childcare items, food and beverage, electronic appliances, furniture, household goods, cosmetics, personal care products, sports and fitness items, and auto accessories.

111. Pinduoduo, originating in China, was designed to compete with prominent Chinese

[33] https://www.wpr.org/news/what-is-temu-and-should-you-let-your-parents-order-from-it#:~:text=Last%20year%2C%20Pinduoduo%20changed%20its,market%20capitalization%20of%20%24169.37%20billion.

online retailers like Alibaba and JD.com, focusing on the sale of budget-friendly goods. The Pinduoduo app functions as a marketplace, enlisting suppliers based in China to offer a variety of cost-effective products to consumers who visit the platform.

112. Previously Pinduoduo was pulled from Google's app store due to the presence of malware that exploited vulnerabilities in the Android operating system to spy on users and competitors. [34]

113. In response to slowing increase in monthly users, Pinduoduo "set up a team of around 100 engineers and product managers to dig for vulnerabilities in Android phones, develop ways to exploit them—and turn that into profit." "By collecting expansive data on user activities, the company was able to create a comprehensive portrait of user's habits, interests and preferences."[35]

114. According to cybersecurity experts, the Pinduoduo App is malware (short for malicious software) because it bypassed "user's cell phone security to monitor activity on other apps, check notifications, read private messages and change settings."[36]

115. Upon information and belief, Defendant used various software, technologies, and programs to covertly intercept, access, and otherwise use Plaintiffs and Class Members' data and information stored on electronic devices.

116. Further, the android analysis report, showed that the code snippets reveal potential

[34] Reuters. "Google suspends China's Pinduoduo app on security concerns." (March 21, 2023). https://www.reuters.com/technology/google-suspends-chinas-pinduoduo-app-due-malware-issues-2023-03-21/

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

[36] I.d.

keylogger activity, as various Android OS build information fields are accessed across different classes and methods. [37] These fields include RELEASE, MODEL, ID, BOARD, BRAND, DEVICE, PRODUCT, FINGERPRINT, TYPE, CPU_ABI, DISPLAY, and more. The extensive access to device details raises concerns about the possibility of keylogging or unauthorized data collection related to users' devices. Defendant's conduct was all performed without the receiving adequate consent from the User.

117. Defendant used various programs and technologies to conduct geo-tracking and other surveillance of Plaintiffs and Class Members, without authorization or permission.

118. More specifically, an analysis of the Temu software by multiple experts who have conducted a detailed examination of the Temu App have determined that it is intentionally designed to conceal its malicious features. The Defendant are alleged to have taken steps to prevent users from discovering the numerous data privacy violations associated with the app. A recent technical analysis uncovered "clues in the software that reflect the app engineers' strong intention to purposefully cloak and obscure what the app actually performs when it is executing."[38]

119. Compiling is the process of creating a computer executable from human-readable code. The Temu App contains "self-compiling software" that circumvents its user's phone's malware detection ability and allows Temu to illegally steal user data.[39]

---

[37] https://www.joesandbox.com/analysis/1337259/0/html

[38] "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" 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/.

[39] The Week. "Why shopping app Temu should be cause for consumer concern." https://theweek.com/china/1026408/temu-consumer-concern-china. (September 11, 2023).

120. Temu uses dynamic compilation using "runtime.exec()". Which calls for "package compile." This built in allows for unbounded use of exploitative methods.[40]

121. Temu's Android cell phone version also intentionally fails to list many of the permissions of its source code in their Android manifest file. The permissions request for the following commands are not listed, despite being the most intrusive: CAMERA, RECORD_AUDIO, WRITE_EXTERNAL_STORAGE, INSTALL_PACKAGES, and ACCESS_FINE_LOCATION. [41]

122. Further, Temu is able to collect any and all files from the user's devices to send to their own servers, with little or no encryption.[42]

123. ACCESS_FINE_LOCATION is a permission for Temu records the precise location rather than the course location whenever the Temu App is running. Temu deceptively requests for users to grant the permission while a photograph is uploaded when an image search is conducted for similar listing.[43]

124. Temu also uses getWindow().getDecorView().getRootView(), to make screenshots and store screenshots as the user uses the smart phone, including the user's activities on other programs and data.[44]

125. Temu references access to the users' camera and microphone whenever the app is using.[45]

126. Temu records both the MAC address and the DNS address.[46]

---

[40] *I.d.*
[41] *I.d.*
[42] *I.d.*
[43] *See* 9.
[44] *I.d.*
[45] *I.d.*
[46] *I.d.*

127. The MAC address is a globally unique identifier of any device in any network, which can be used to identify the owner.[47]

128. Temu asks for the MAC address and inserts it into a JSON object to be sent to the server.

129. Temu seeks "root" access of the cell phone, which includes not only the files on the application, but all files on the device, including the programming of the other apps and the operating system.[48]

130. Temu's code references the system log files' address and options for shell commands.[49]

131. Temu obfuscates its app behavior through cleanup tools and debugger applications that makes it very difficult.[50]

132. Joe Security, an ISO 27001 certified company which specializes in the development of malware analysis systems for malware detection and forensics, rates Temu's app with 68/100, a score that is even higher than the malicious Pinduoduo app, which was suspended from the app store.[51]

133. Like their parent's malware, Pinduoduo, Temu's app is almost identically malicious in the categories: Spyware, Evader, and exploiter.[52]

134. Further, the analyzed report indicates that the submitted APK (Android application package) has permissions and capabilities related to key, mouse, clipboard,

---

[47] *Media Access Control Address (MAC Address)*, Techopedia (Nov. 18, 2014), available at https://www.techopedia.com/definition/5301/media-access-control-address-mac-address (last visited Nov. 8, 2022).
[48] *I.d.*
[49] *I.d.*
[50] *I.d.*
[51] *I.d.*
[52] *I.d.*

microphone, and screen capturing[53]. Specifically:

a. *Audio Recording Permission*: The app has requested permission to record audio in the background (android.permission.RECORD_AUDIO). It utilizes various sources and API calls, such as android.media.AudioRecord.startRecording, indicating that it is capable of recording audio.

b. *Camera Permission*: The app has requested permission to take photos (android.permission.CAMERA), suggesting that it can access the device's camera functionality.

c. *Audio/Media Recording Actions*: The app engages in audio/media recording activities, as evidenced by API calls like android.media.AudioRecord.startRecording in different source locations, indicating potential audio recording capabilities.

d. *Modification of Audio Routing Behavior*: The app modifies the audio routing behavior through API calls to android.media.AudioManager.setMode, specifically in the context of the xmg.mobilebase.audio.audioenginesdk.enginesession.AudioEngineSession class.

e. *Access to Audio/Media Managers*: The app accesses audio/media managers, as indicated by references to android.media.AudioManager in the source code.

135. Overall, the summarized report suggests that the analyzed APK has permissions and functionalities related to capturing audio, taking photos, and potentially manipulating audio routing behavior on the device. These capabilities should be considered in the

[53] https://www.joesandbox.com/analysis/1321798/0/html

context of the app's intended functionality and user privacy concerns.

***d. User Data and Data Breach***

136. Temu App analysis shows that Defendant's exhibit a behavior associated with stealing sensitive information from user's device[54]. Here are some of the key points from the analysis report:

a. *Device Information*: Reads the serial number of the device using the method ro.serialno in the class xmg.mobilebase.secure.c.

b. *SIM Card Detection*: Checks if a SIM card is installed by invoking android.telephony.TelephonyManager.getSimState in the class xmg.mobilebase.secure.c.

c. *Media Storage Queries*: Queries the media storage location field using the android.provider.MediaStore$Images$Media.EXTERNAL_CONTENT_URI in various classes like ay.a, ay.b, ay.k, com.einnovation.whaleco.album.jsphoto.ImagePhotoPicker.

d. *Installed Packages*: Queries the list of installed packages through android.content.pm.PackageManager.getInstalledPackages in the class xmg.mobilebase.secure.c.

e. *Logcat Reading*: Reads the logcat using java.io.BufferedReader.readLine in the class ap.b.

f. *Receiver Priority*: Has an unnatural receiver priority for android.intent.action.BOOT_COMPLETED, which is often an indicator for malware (0x7fffffff).

[54] https://www.joesandbox.com/analysis/1321798/0/html

g. *Camera Operations*: May take a camera picture, evidenced by the usage of android.media.action.IMAGE_CAPTURE intent in classes like androidx.activity.result.contract.ActivityResultContracts$TakePicture, com.einnovation.whaleco.album.jsphoto.ImagePhotoPicker,com.einnovation.whaleco.album.jsphoto.PhotoV2Presenter.

h. *Clipboard Monitoring*: Registers a clipboard change listener through android.content.ClipboardManager.addPrimaryClipChangedListener in the class sr.a.

i. *Installed Applications*: Queries a list of installed applications via android.content.pm.PackageManager.queryIntentActivities in the class com.baogong.router.pinbridge.AMNavigator.

j. *Account Information*: Queries stored mail and application accounts (e.g., Gmail or WhatsApp) by invoking android.accounts.Account.name in classes like ak.a, cj.d, com.google.android.gms.auth.api.signin.GoogleSignInOptions.

k. *WiFi Access Points*: Queries the list of configured WiFi access points using android.net.wifi.WifiManager.getConfiguredNetworks in classes like com.einnovation.temu.appinfo.task.AppStatSSIDTask, xmg.mobilebase.secure.c.

l. *Camera Information*: Queries camera information through android.hardware.Camera methods in classes like jv.b, jv.a, oo.j.

137. These behaviors indicate potential data theft, including device identification, SIM card presence, media storage details, installed packages, logcat reading, receiver priority manipulation, camera operations, clipboard monitoring, account information retrieval,

WiFi access point details, and camera information queries.

138. A more detailed explanations of the android analysis report exhibits that the Temu App, contains functionalities that check for popular installed apps and has the capability to add an overlay to other apps[55]. Here's a summary:

j. Checking for Popular Installed Apps:

i. **Class**: Lcom/baogong/app_baog_share/JSBGShare

ii. **Method**: collectAvailableChannels

iii. **Checked Apps**:

"com.facebook.katana"
"com.facebook.orca"
"com.whatsapp"
"com.twitter.android"
"com.snapchat.android"
"com.instagram.android"

**Purpose**: The code appears to check for the presence of popular social media and messaging apps on the device. This information could potentially be used for various purposes, including targeting users of these apps for fraudulent activities.

k. Overlay Functionality:

i. **Class**: dn1.b

ii. **Method**: b

iii. **API Call**: WindowManager.addView

iv. **Purpose**: The code contains functionality related to adding an overlay to other apps. Adding overlays can be a technique used to create phishing overlays or fake login screens on top of legitimate applications, aiming to

[55] https://www.joesandbox.com/analysis/1337259/0/html

trick users into providing sensitive information.

**Caution**: The identified behavior, especially the overlay functionality, raises concerns about the potential involvement in fraudulent activities, such as phishing or attempting to deceive users of banking or social media apps. It is crucial to thoroughly review and investigate the context and purpose of these functionalities to ensure the security of users and prevent malicious activities.

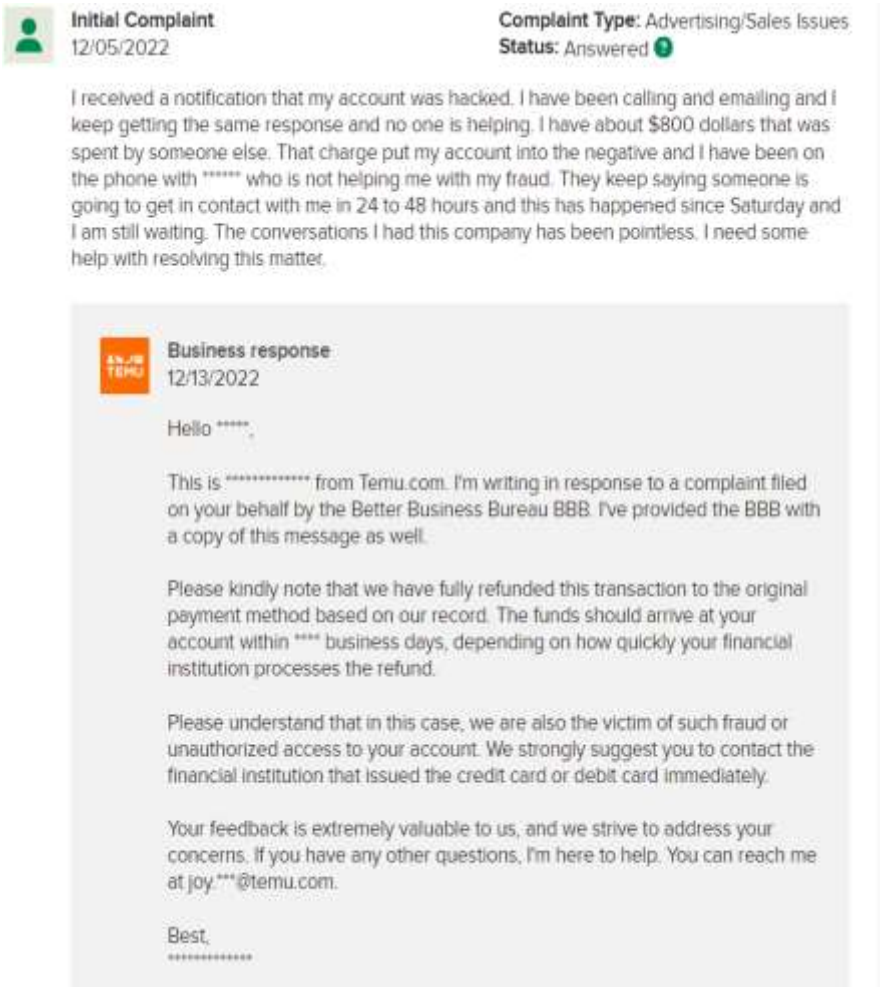
***e. Defendant failure to notice the Plaintiffs and its App Users of Potential Data Breach despite Multiple Reportings made by the App Users:***

139. Plaintiff Nancy Batalas installed and began using the Temu App, only to encounter a series of unauthorized cash deductions from her checking account, totaling $1,500.00 and $600.00. Upon discovering this alarming situation, Ms. Batalas was forced to allocate her time and effort to address the aftermath. She had to undergo the inconvenience of closing her compromised checking account to prevent further unauthorized transactions. To her dismay, she also uncovered that the hackers had exploited her personal information to open a sapphire credit card account in her name. Consequently, Ms. Batalas had to dedicate additional time to rectify this issue by closing the fraudulent credit card account. The ordeal highlights the significant disruptions and distress caused by the unauthorized access to her financial accounts, underscoring the urgent need for improved security measures and accountability within the Temu platform.

140. Upon information and belief, Ms. Batalas claims that she previously had not suffered any type of fraud, identify theft or phishing before the Data Breach. Ms. Batalas further claims that, it was only after she started using the services of the Defendant's shopping app, she started experiencing fraudulent bank transfers.

141. Additionally, a closer look at the list of complaints raised by Temu App users against

Defendant's in Better Business Bureau (*herein referred as* "BBB") website shows that Defendant's received several complaints from app users stating their credit/debit cards were illegally charged. Some of the App users went on to further state that, some hackers even used their cards to make purchases at the Temu website. For several of the reimbursement request made by the app users, Temu's part of the standard response was "*Please understand that in this case, we are also the victim of such fraud or unauthorized access to your account. We strongly suggest you to contact the financial institution that issued the credit card or debit card immediately*."



**Initial Complaint**
12/05/2022

**Complaint Type:** Advertising/Sales Issues
**Status:** Answered

I received a notification that my account was hacked. I have been calling and emailing and I keep getting the same response and no one is helping. I have about $800 dollars that was spent by someone else. That charge put my account into the negative and I have been on the phone with ****** who is not helping me with my fraud. They keep saying someone is going to get in contact with me in 24 to 48 hours and this has happened since Saturday and I am still waiting. The conversations I had this company has been pointless. I need some help with resolving this matter.

**Business response**
12/13/2022

Hello *****,

This is ********** from Temu.com. I'm writing in response to a complaint filed on your behalf by the Better Business Bureau BBB. I've provided the BBB with a copy of this message as well.

Please kindly note that we have fully refunded this transaction to the original payment method based on our record. The funds should arrive at your account within **** business days, depending on how quickly your financial institution processes the refund.

Please understand that in this case, we are also the victim of such fraud or unauthorized access to your account. We strongly suggest you to contact the financial institution that issued the credit card or debit card immediately.

Your feedback is extremely valuable to us, and we strive to address your concerns. If you have any other questions, I'm here to help. You can reach me at joy.***@temu.com.

Best,
**********

**Initial Complaint**
12/29/2022

**Complaint Type:** Problems with Product/Service
**Status:** Answered

I have been trying to speak to Temu in regards to an order that was fraudulently made on my Temu account and trying to request a refund to my financial institution immediately as I made a very stupid decision to hook my PayPal account to my Temu account which then made check out fast and easy well a order was placed on my Temu that has my name on it and a different address and they keep telling me to wait for the goods to arrive but I reply with what good does this do for me like I wont be receiving them to like ship it back for a refund so why would I wait for the goods to be delivered I just want my ****** Ive spoke to so many people in the chat its unreal Ive been lied to told by 4 people they are getting the supervisor then if I actually did get a supervisor they claim to send it to escalations to be handled in ***** hrs and then one claimed they fwd to the head office and some say again I am going to get my supervisor but leaving this chat open so when I reply back to see whats going on I get a new person who then all of a sudden know nothing about this want to know what order and feeds me the run around literally they dont have a fraud department they dont have good and effective customer service they have no morals as a company how they can provide a service that allows your financial institution to be linked to Temu for payment and then have absolutely no department for a customer to take exchange their concerns for a resolution and after making 2 phone calls and being lied to about how they want to handle it and that they are going to refund it and me following up and finding out its a lie Im now sticking to the chat version only so I can have visual proof of this due to the **** poor customer services and this last chat I was in they finally asked me my address I gave it Then asked for my phone# and I said Im sorry but no you cant have my number you can reach me via chat as I will have proof if Im lied to again cause I was filing this w bbb

**Business response**
12/11/2022

Hello ******,

This is ********** from Temu.com. I'm writing in response to a complaint filed on your behalf by the Better Business Bureau BBB. I've provided the BBB with a copy of this message as well.

Please kindly note that we have fully refunded this transaction to the original payment method based on our record. The funds should arrive at your account within 5-7 business days, depending on how quickly your financial institution processes the refund.

Please understand that in this case, we are also the victim of such fraud or unauthorized access to your account. We strongly suggest you to contact the financial institution that issued the credit card or debit card immediately.

Your feedback is extremely valuable to us, and we strive to address your concerns. If you have any other questions, I'm here to help. You can reach me at joy.***@temu.com.

Best,
**********

**Initial Complaint**
12/05/2022

**Complaint Type:** Problems with Product/Service
**Status:** Answered

I have 7 withdrawals from Temu.com on my account and have never purchased or received anything from this site. I have never even heard of the site until I saw the charges on my account today. The charges are for ***** (11/23/22), ***** (11/23/22), ***** (11/24/22), ***** (11/26/22), **** (11/27/22), ***** (11/27/22), and ***** (11/28/22) for a total of ******. I need my money back because this is fraudulent activity that was not authorized. My bank has been made aware of the fraudulent charges as well.

**Business response**
12/13/2022

Hello Raeshon,

This is ********** from Temu.com. I'm writing in response to a complaint filed on your behalf by the Better Business Bureau BBB. I've provided the BBB with a copy of this message as well.

Please kindly note that we have fully refunded this transaction to the original payment method based on our record. The funds should arrive at your account within **** business days, depending on how quickly your financial institution processes the refund.

Please understand that in this case, we are also the victim of such fraud or unauthorized access to your account. We strongly suggest you to contact the financial institution that issued the credit card or debit card immediately.

Your feedback is extremely valuable to us, and we strive to address your concerns. If you have any other questions, I'm here to help. You can reach me at joy.***@temu.com.

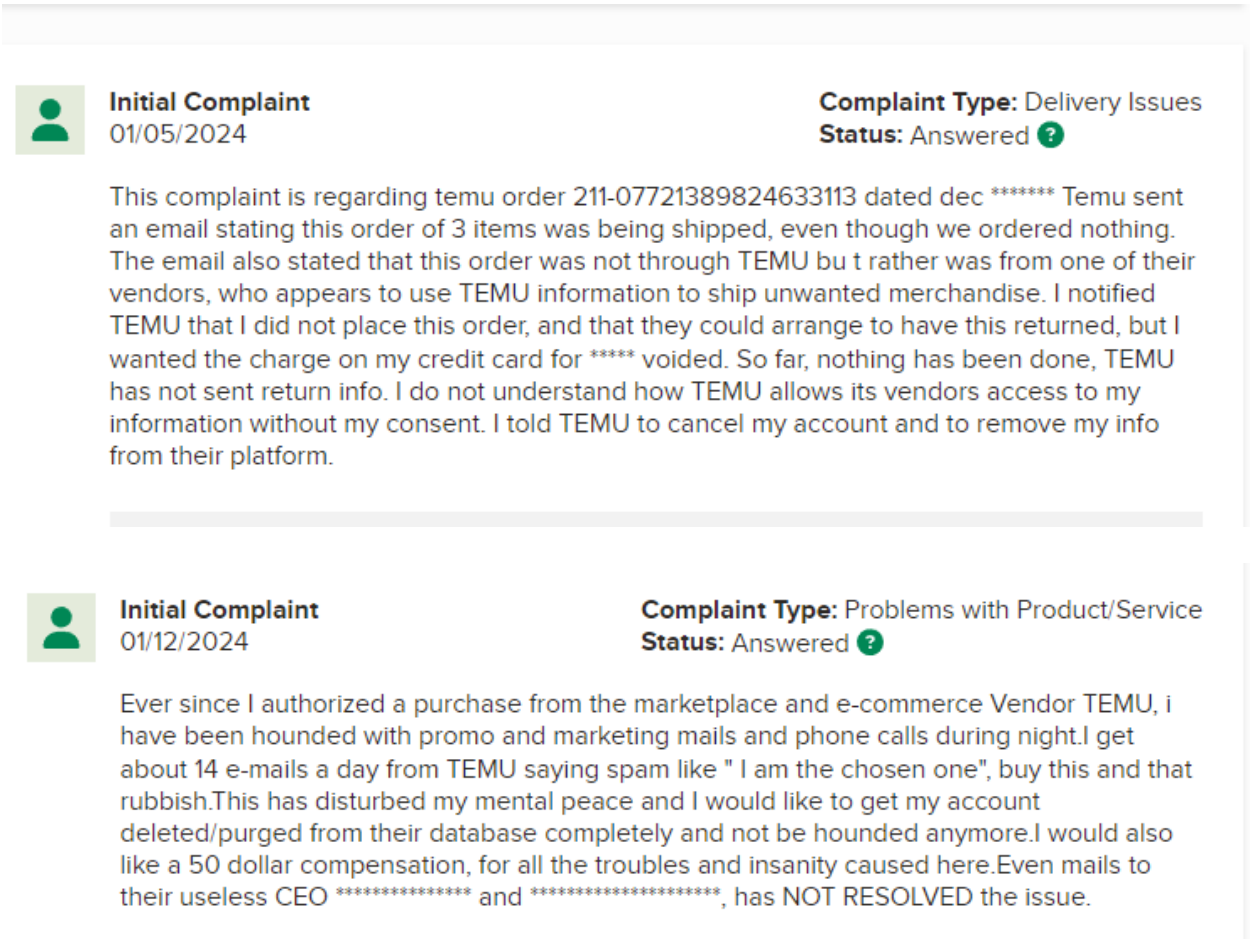
Best,
**********

**Customer response**
01/11/2024

Better Business Bureau:I have reviewed the response submitted by the business and have determined that the response does not satisfy or resolve my issues and/or concerns in reference to complaint # ********. Please add your rejection comments below; if you do not provide any details, your complaint will be closed as Answered.
**[You must provide details of why you are not satisfied with this resolution. If you do not enter a reason for your rejection, your complaint will be closed as Answered.]**
again, when Temu advised me that this order was in process, it also stated that this was not an order from Temu but rather an order processed on their platform from one of its vendor partners, and it also asked if I in fact had placed this order. I thought this was odd, that Temu did not know if I had or had not placed this order. And I i in fact did not place this order, and so advised Temu. Nevertheless the merchandise was delivered and my credit card was billed. How TEMU allowed one of its vendor partners to access my information, including my credit card, is beyond me. Needless to say, based on review of other complaints on the BBB website, I am not alone. I also asked TEMU to cease sending email offers and to remove my information from their server, but I am still receiving offers And for the record, I asked my credit card company to dispute the charge, which they agreed to without question.
Businesses and Customers should be civil, courteous and polite in their responses to complaints. It is important to remain professional and productive when participating in the BBB complaint process.

FAQ

Regards,f
****



**Initial Complaint**
01/05/2024

**Complaint Type:** Delivery Issues
**Status:** Answered

This complaint is regarding temu order 211-07721389824633113 dated dec ******* Temu sent an email stating this order of 3 items was being shipped, even though we ordered nothing. The email also stated that this order was not through TEMU bu t rather was from one of their vendors, who appears to use TEMU information to ship unwanted merchandise. I notified TEMU that I did not place this order, and that they could arrange to have this returned, but I wanted the charge on my credit card for ***** voided. So far, nothing has been done, TEMU has not sent return info. I do not understand how TEMU allows its vendors access to my information without my consent. I told TEMU to cancel my account and to remove my info from their platform.

**Initial Complaint**
01/12/2024

**Complaint Type:** Problems with Product/Service
**Status:** Answered

Ever since I authorized a purchase from the marketplace and e-commerce Vendor TEMU, i have been hounded with promo and marketing mails and phone calls during night.I get about 14 e-mails a day from TEMU saying spam like " I am the chosen one", buy this and that rubbish.This has disturbed my mental peace and I would like to get my account deleted/purged from their database completely and not be hounded anymore.I would also like a 50 dollar compensation, for all the troubles and insanity caused here.Even mails to their useless CEO ********** and **********, has NOT RESOLVED the issue.

142. While Temu does offer reimbursement to customers affected by fraudulent activities in their bank accounts, the failure to notify app users about potential breaches remains a significant concern. Numerous complaints from app users highlight instances where unauthorized charges have occurred without any corresponding action or communication from Temu regarding the breach. This lack of proactive disclosure not only undermines trust in the platform but also leaves users unaware of potential security risks they may face. Addressing this issue requires Temu to prioritize transparency and promptly inform users of any breaches, empowering them to take necessary precautions to protect their financial information. Failure to do so not only pose a risk to users but also reflects poorly on Temu's commitment to safeguarding customer data. Thus, while

reimbursement offers a form of redress, it must be coupled with proactive measures to notify and educate users about potential breaches to uphold trust and security within the platform.

***f. Temu Contains Spyware and Actively Collects User Information:***

143. According to a September 13, 2023, NBC Chicago Report, entitled "Using TEMU could expose consumers to identity theft, other issues," [56] the Better Business Bureau warns that "the app collects a lot of information from consumers, including your social media and banking information. Cyber security experts say they suspect the app could even bypass cellphone security settings to spy on other apps and even change settings.[57]"

## I. TEMU FACES USA SCRUTINY ALONGSIDE WECHAT, CAPCUT, SHEIN, AND ALIEXPRESS: PRIVACY CONCERNS AND ALLEGATIONS OF HUMAN RIGHTS VIOLATIONS:

144. As concerns over data privacy and national security intensify, there is a heightened scrutiny of mobile apps in the United States. The recent decision to prohibit Temu App on government devices serves as a notable illustration of this trend, prompting discussions about how Temu could be the next app that may be flying under the radar and could potentially face nationwide restrictions.

***a. Temu Shares User Data with Unauthorized Third Parties:***

145. As repeatedly noted by experts and government authorities, user data owned by Chinese companies is readily accessible to officials of the Chinese communist government under applicable law. The Chinese government has well-documented,

[56] https://www.nbcchicago.com/consumer/bbb-using-temu-could-expose-consumers-to-identity-theft-other-issues/3227474/
[57] *i.d.*

continuous efforts to obtain private user data from American citizens, employing both legal and illegal means.

146. In October 2019, United States Senators Charles Schumer and Tom Cotton took bipartisan action by sending a letter to the Acting Director of National Intelligence. The letter outlined the potential risks associated with Chinese ownership of the Temu App. Despite Temu App's assertion that it does not operate in China and stores U.S. user data within the U.S., the Senators emphasized a significant security risk. This concern stemmed from the fact that Temu App, as a Chinese-owned entity, was still obligated to adhere to the laws of China, raising apprehensions about the handling of user data. As the Senators explained, "Security experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party."[58]

147. On November 15, 2020, a CBS News 60 Minutes broadcast highlighted the risks associated with Chinese ownership of companies that gather private and personally identifiable information from American users. The broadcast featured insights from a former member of the U.S. intelligence community, who noted that the possession of U.S. user data by China-affiliated companies is particularly alarming. This concern was underscored by the observation that the Chinese government and industry have amalgamated, collaborating closely to pursue state objectives. As Senator Hawley observed during the broadcast, for example, the Chinese-owned parent company of

[58] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-nationalsecurity-threats;
https://www.cotton.senate.gov/?p=press_release&id=1239.

Temu App had an express legal obligation to share such private user data with the Chinese government: "under Chinese law, Temu App, ByteDance, the parent, is required to share data with the Chinese Communist Party"; "all it takes is one knock on the door of their parent company, based in China, from a Communist Party official for that data to be transferred to the Chinese government's hands, whenever they need it."[59]

148. In testimony given to Congress in November 2022, FBI Director Christopher Wray reiterated these concerns, noting that Chinese law requires Chinese companies to "do whatever the government wants them to in terms of sharing information or serving as a tool of the Chinese government." "And so that's plenty of reason by itself to be extremely concerned."[60]

149. Based on such concerns, Senator Marco Rubio and Representative Mike Gallagher recently introduced legislation to completely ban Temu App "and other social media companies that are effectively controlled by the CCP [Chinese Communist Party] from operating in the United States.". [61]There have been similar calls for specific action against Temu by commentators who argue that "TEMU is demonstrably more dangerous than Temu App. The app should be removed from the Google and Apple

[59] https://www.nbcnews.com/politics/congress/hawley-takes-aim-tiktok-china-congressionalhearing-n1076586.
[60] https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china.
[61] https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china; *see also* https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-tiktok-americachina- mike-gallagher/.

app stores.".[62]

150. In the pursuit of advancing its artificial intelligence technologies, the Chinese government has endeavored to amass large quantities of user data, encompassing biometric information. As the South China Morning Post reported: "China's goal of becoming a global leader in artificial intelligence (AI) is nowhere more manifested than in how facial recognition technology has become a part of daily life in the world's second-largest economy. Facial recognition systems, which are biometric computer applications that automatically identify an individual from a database of digital images, are now being used extensively in areas such as public security, financial services, transport and retail across the country." [63]In fact, the Chinese government employs a variety of biometrics for population surveillance and control: "In addition to voice recognition, there are facial and pupil recognition, gathering of DNA samples—building the world's largest DNA database—and fingerprint scans."[64]

151. Artificial intelligence algorithms feed on data to learn and improve – thus, the more data, the better the development of the algorithms driving the advance of the artificial intelligence. [65] With better artificial intelligence comes more effective population surveillance and control.

152. To advance these interrelated goals, the Chinese government has worked hand in glove

[62] https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shoppingapp-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/
[63] https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushingfacial-recognition-technology.
[64] https://brandscovery.com/business/content-2254742-china-gathers-people-s-voices-newidentification-technology-drawing-concerns.
[65] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/

with China-based technology companies to accumulate and share data. For example, the China-based company Megvii, a leader in computer vision, has the world's largest open-source database (Face++) for training other facial recognition algorithms. It has reportedly used government data banks to help compile this training program. [66] Similarly, the Chinese government partnered with the China-based technology firm d-Ear Technologies to build a database of voiceprints for voice recognition purposes.[67]

153. "Private [China-based] corporations and the [Chinese] Communist Party's security apparatus have grown together, discovering how the same data sets can both cater to consumers and help commissars calibrate repression. … Many [China-based] tech firms make a point of hiring the relatives of high party officials, and a vast state database of headshots might be shared with a private firm to train new facial recognition software, while the firm's trove of real-time user data might be offered to police, for a panoramic view of potential 'troublemakers.'"[68]

154. Such data gathering is not confined to China's borders. The Chinese government is compiling a tremendous storehouse of private and personally identifiable data on ordinary Americans. For example, Chinese government-sponsored hackers stole data belonging to approximately 500 million Marriott International guests. "[M]achine learning is yielding uses for large data sets that humans alone could not imagine – or even understand – given that machine learning can generate correlations among data

[66] *I.d.*
[67] https://brandscovery.com/business/content-2254742-china-gathers-people-s-voices-newidentification-technology-drawing-concerns
[68] https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberalinnovation.
html.

that the machine itself can't explain. … Beijing's plan may be simply to vacuum up as much data like this as possible and then see what today's machine learning—or, better yet, tomorrow's machine learning—can do with it."[69]

155. The lengths to which the Chinese government will go to obtain such data about ordinary Americans is further evidenced by other large-scale hacking schemes, including one involving 145 million Americans whose data was held by Equifax, [70] and another involving 78 million Americans whose data was held by Anthem. [71] "The United States assessed that China was building a vast database of who worked with whom in national security jobs, where they traveled and what their health histories were, according to American officials. Over time, China can use the data sets to improve its artificial intelligence capabilities to the point where it can predict which Americans will be primed for future grooming and recruitment …." [72] "The hacks, security researchers said, were an extension of China's evolving algorithmic surveillance system, which has greatly expanded over the past few years." [73] Frequently, Chinese-based hacking against the U.S. has been tied specifically to the Chinese military.[74]

156. In cases like this, where Chinese-owned technology companies, such as the Defendant, have covertly accumulated such data independently, there is no requirement for the Chinese government to resort to hacking for data acquisition. According to Chinese law, this information is directly accessible to them.

---

[69] https://www.justsecurity.org/62187/weapons-mass-consumerism-china-personalinformation/.
[70] https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html
[71] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html.
[72] https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html.
[73] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html.
[74] https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to hackingagainst-us.html.

157. That is because such China-based companies are required by law to secretly provide that data to the government upon demand:

> The message contained in each of China's state security laws passed since the beginning of 2014 is clear: everyone is responsible for the party-state's security. According to the CCP's definition of state security, the Party's political leadership is central. … And the party expects Chinese people and citizens to assist in collecting intelligence. The Intelligence Law states "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of…" Not only is everyone required to participate in intelligence work when asked, but that participation must be kept secret.[75]

158. Chinese law requires Chinese citizens, and individuals and organizations or entities in China, to cooperate with "national intelligence work." It grants Chinese government and Communist Party officials broad, invasive authority to, among other things, access private networks, communications systems, and facilities to conduct inspections and reviews. These laws are broad and open-ended. 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."[76]

159. The concerns with transferring personal data from U.S. users to Chinese-based companies that was raised recently TikTokApp and Temu are so great that Congress

[75] https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/.; *See also* https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

[76] M. Scot Tanner, Beijing's New National Intelligence Law: From Defense to Offense, LAWFARE (July 20, 2017), https://bit.ly/3fXfB4A

has drafted legislation that would prohibit the transfer of personal data from users in the United States to entities or individuals that are under the control or influence of China such as China-affiliated businesses like Temu App and Temu.[77]

160. The documented data privacy violations associated with the Temu App are especially alarming, not just because they involve the unauthorized collection and potential sale of user data to third parties. What adds to the concern is the fact that Temu's parent company PDD Holdings, is based in China and is bound by Chinese law, which mandates companies to furnish user data to the government upon request. Further, as a technical analysis of the Temu App has noted, "Your personal data – much more than you ever assumed – is resold indiscriminately for marketing purposes, and in all probability available to Chinese Security authorities for data mining purposes. Chinese Government security agents or their AI computers might be looking at what products you or your family buy on TEMU as a source of leverage, influence, manipulation, 'cross-border remote justice', surveillance, or more."[78]

## J. DEFENDANT'S PRIVACY POLICIES DO NOT CONSTITUTE NOTICE OF OR CONSENT TO THE TRANSFER OF PRIVATE AND PERSONALLY IDENTIFIABLE DATA AND CONTENT TO SERVERS IN CHINA:

### a. *Deficiencies in Temu's Privacy Policy and Ambiguities in Data Handling Disclosures*:

161. Temu's users certainly do not provide informed consent to Defendant's privacy policies due to insufficient display of notice and warnings, as previously discussed. Moreover, numerous provisions within the privacy policies are ambiguous, offering inadequate clarity regarding the nature of the private and personally identifiable user data and

[77] https://www.congress.gov/bill/118th-congress/house-bill/1153/text
[78] 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/

content being collected and its destination. Even experts in the field can find it challenging to discern the specifics of what is being collected and where it is being sent. Given this complexity, it is unreasonable to expect ordinary Temu users to comprehend these perplexing "disclosures." The lack of clarity in these policies contributes to the inadequacy of notice, making it difficult to infer knowing user consent.

162. In addition to the mentioned deficiencies, privacy policy provisions indicating that specific Temu user data and content might be transmitted to servers in China contradict Defendant's public and deceptive assurances that no such transfers take place. Furthermore, Temu users, whose data and content are sent before they have a chance to sign up and create an account, do not effectively or implicitly receive notice. Consequently, they cannot be considered to have given their assent to such transfers to China.

163. Defendant's privacy policy explicitly states that the information collected from Temu users will be shared with its affiliates and other service providers. Additionally, the Privacy Policy specifies that the user data collected may be transferred to locations outside of the United States, where privacy laws may not provide the same level of protection as those in the user's state, province, or country.

164. The privacy policy displayed on Defendant's website, last updated on March 22, 2023, outlines how Defendant handles users' personal information. Notably, the privacy policy, without disclosing its affiliation with PDD Holdings, mentions the following: "Whaleco Inc., and its affiliates (“Temu”, “we”, “us” or “our”) handles personal information that we collect through our digital properties that link to this Privacy &

Cookie Policy, including our website (www.temu.com), the Temu mobile application and Temu's seller portal (collectively, the "Service"), as well as through social media, our marketing activities, and other activities described in this Privacy and Cookie Policy."

165. Starting approximately in April 2023, Defendant Temu's website ceased to disclose any affiliation with PDD Holdings. The Temu website now exclusively highlights that its business is founded and operated in Boston, Massachusetts, since 2022, without making any mention of its association with PDD Holdings anywhere on the website. This omission becomes an additional factor contributing to users being unaware that their data may be transmitted to China without their knowledge.

166. Moreover, as the privacy policy discloses, the Defendant's transmission of user data to its affiliates, third parties, or its parent company PDD Holdings raises significant concerns, particularly in the context of an elevated risk of providing information about United States Citizens, even without a valid warrant or subpoena issued by a court of competent jurisdiction. To clarify, the Chinese government does not possess competent jurisdiction over Temu's U.S. users. Therefore, Temu's action of transmitting the user's personal and private information outside of the United States or to its affiliates or third parties does not comply with legal standards.

## K. TEMU PROFITS WHILE PLAINTIFFS AND THE CLASS MEMBERS SUFFER HARM:

167. As explained previously, Defendant covertly carried out several actions, during the period when the Temu App was installed on the mobile devices of the named plaintiffs and the class members, without providing notice or obtaining the knowledge and consent of the named plaintiffs, and in the case of the minor class plaintiffs, without

the consent of their legal guardians. These actions included: (i) collecting plaintiffs' biometric identifiers and information from their mobile devices; (ii) extracting user/device identifiers and private data from plaintiffs' mobile devices; (iii) acquiring plaintiffs' private and personally identifiable data and content from their mobile devices; and (iv) enabling access to some or all of the stolen data and content by individuals in China, including those under the control of the Chinese government.

168. Defendant engaged in these actions with the intention of covertly gathering the private and personally identifiable data and content of the named plaintiffs and the class members. This includes user/device identifiers, biometric identifiers and information, and other private details. The objective behind these actions was to track, profile, and target plaintiffs and the class members with advertisements. Moreover, Defendant has utilized plaintiffs' and the class members private and personally identifiable data and content for their economic gain. Defendant and other entities now have access to private and personally identifiable data and content related to the plaintiffs and the class members, which can be exploited for further commercial advantages and potentially harmful purposes. Defendant has already profited from these activities, and it is anticipated that they will continue to do so.

169. Additionally, the named plaintiffs and the class members have experienced harm due to Defendant's infringement on their privacy rights through the clandestine acquisition of their private and personally identifiable data and content. This includes their user/device identifiers, biometric identifiers and information, and other private data. Plaintiffs and the class members have also suffered harm because Defendant's actions have devalued their private and personally identifiable data and content. Furthermore,

plaintiffs and the class members have experienced damage to their mobile devices, with the battery, memory, CPU, and bandwidth being compromised. As a result, the functionality of these devices has been impaired and slowed down due to Defendant's covert and unlawful activities. Finally, plaintiffs and the class members have incurred additional data usage and electricity costs that they and/or their guardians would not have borne were it not for Defendant's covert and unlawful actions.

170. Neither the named plaintiffs, the Class (including the minor class members and in case of minor class member their guardians), received any notice that Defendant would collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers and other private information. Defendant did not inform plaintiffs or their guardians about the specific purpose and duration for which their biometric identifiers or other biometric information would be collected, captured, received, otherwise obtained, stored, and/or used. Additionally, neither the Plaintiffs nor, in the case of minors, their guardians, ever signed a written release authorizing Defendant to collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers or other biometric information.

171. According to counsel's investigation and analysis, Temu intentionally crafted its Terms of Service and Privacy Policy in a way that diminishes the likelihood of users noticing and comprehending its terms and conditions. This design aims to hinder users from providing meaningful, express consent to its conditions, intending to encourage users to sign up without being deterred by accurate and truthful disclosures.

172. The named plaintiffs and the class members were unaware and did not anticipate that Defendant would collect, store, and utilize their biometric identifiers and biometric

information while using the Temu App.

173. The named plaintiffs and the class members did not receive any form of notice from Defendant's, whether written or otherwise, regarding the collection, storage, and/or usage of their biometric identifiers or biometric information. Defendant's failed to inform plaintiffs and the class members of the specific purpose and duration for which they would collect, store, and/or use their biometric identifiers or biometric information. Additionally, plaintiffs and the class members did not provide authorization, whether written or otherwise, for Defendant to collect, store, and/or use their biometric identifiers or biometric information.

## CLASS ACTION ALLEGATIONS

174. Plaintiff brings Count I and IV, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in the United States who registered an account with Temu at any time from July 2022 to the present day (the "National Class").

175. Excluded from the National Class, are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

176. Plaintiffs bring Count II, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[79] who registered an account with Temu e-grocery service at any time from July 2022 to the present day (the "Consumer Fraud Multistate Class").

177. Excluded from the Consumer Fraud Multistate Class, are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

178. In the alternative to Count II, Plaintiff brings Count III, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of the following state sub-class, defined as:

> All persons residing in the State of New York who registered an account with Temu e-grocery service at any time from July 2022 through the present day (the "New York State Class").

179. Excluded from the New York State Class, are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers.

---

[79] The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code § 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq*.); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq*.); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq*.); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.* ); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq*.); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349,*et seq*.); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania (73 P.S. § 201-1, *et seq*.); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6- 101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

180. The National Class, Consumer Fraud Multistate Class, and New York State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

181. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

***NUMEROSITY***

182. The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands to millions. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Defendant's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

***COMMONALITY AND PREDOMINANCE***

183. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Temu failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive personal information;

b. Whether Temu properly implemented its purported security measures to protect customer information from unauthorized capture, dissemination, and misuse;

c. Whether Defendant's conduct violates the New York and other asserted Consumer Fraud Acts;

d. Whether Defendant's conduct constitutes breach of an implied contract;

e. Whether Defendant violated the Federal Wire Tap Act, 18 U.S.C. §§ 2510, *et seq*.;

f. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

184. Temu engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

***TYPICALITY***

185. Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the Breach alleged herein. Further, there are no defenses available to Temu that are unique to Plaintiffs.

***ADEQUACY OF REPRESENTATION***

186. Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

***INSUFFICIENCY OF SEPARATE ACTIONS***

187. Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would

cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Temu. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

***DECLARATORY AND INJUNCTIVE RELIEF***

188. Temu has acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

***SUPERORITY***

189. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Temu, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## CAUSES OF ACTION

**COUNT I. Negligence**
**(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)**

190. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

191. Plaintiffs bring this claim individually and on behalf of the nationwide Class.

192. Defendant knowingly collected, came into possession of and maintained Plaintiffs' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

193. Defendant had and continues to have a duty to timely disclose that Plaintiffs' Private Information within its possession might have been compromised and precisely the types of information that were compromised.

194. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' Private Information.

195. Defendant systematically failed to provide adequate security for data in its possession.

196. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' Private Information within Defendant's possession.

197. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' Private Information.

198. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class members the fact that their Private Information within

its possession might have been compromised and precisely the type of information compromised.

199. Defendant's breach of duties owed to Plaintiffs and the Class proximately caused Plaintiffs' and Class Members' Private Information to be compromised.

200. As a result of Defendant's ongoing failure to notify consumers regarding what type of PII has been compromised, consumers are unable to take the necessary precautions to mitigate their damages by preventing future fraud.

201. Defendant's breaches of duty caused Plaintiffs to overpay for goods, purchase goods they would not otherwise have purchased, suffer fraud on their credit or debit cards, identity theft, phishing, temporary loss of use of their debit cards and access to the funds therein, loss of time and money associated with resolving the fraudulent charges on their cards, loss of time to monitor and cancel additional cards or accounts, loss of time and money monitoring their finances for additional fraud, diminished value of the services they received, and loss of control over their PCD and/or PII.

202. As a result of Defendant's negligence and breach of duties, Plaintiffs' Private Information was compromised, obtained by a third party, and used by a third party to cause Plaintiffs Starlings and Batalas to incur fraudulent charges, to spend time clearing up those charges, and to be without the use of their debit and credit cards for a period of time.

203. Additionally, Plaintiffs are in danger of imminent harm that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

204. Plaintiffs seek the award of actual damages on behalf of the Class.

205. In failing to secure Plaintiffs' and Class Members' Private Information and promptly

notifying them of the Data Breach, Defendant was guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

206. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the data breach.

**COUNT II. Breach of Implied Contract**
**(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)**

207. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

208. Defendant required customers who intended to make In Store Purchases with debit or credit cards to provide their cards' magnetic strip data for payment verification.

209. In providing such information, Plaintiffs and other Class members entered into an implied contract with Defendant Whereby Defendant became obligated to reasonably safeguard their sensitive and non-public information.

210. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard their financial data.

211. Plaintiffs and Class Members suffered and will continue to suffer damages including, but not limited to, actual identity theft, fraud and/or phishing, loss of money and costs incurred as a result of increased risk of identity theft, and loss of their PCD and PII,

all of which have ascertainable value to be proved at trial.

**COUNT III. Unjust Enrichment**
**(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)**

212. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

213. Plaintiffs hereby plead in the alternative to the Second Count.

214. The common law prohibits Defendant from reaping a substantial financial profit at the expense of Plaintiffs and the other Class Members' expense without reasonable and equitable restitution

215. Defendant reaped a significant financial profit from its system of monitoring the Internet connections on the subject computers or cellphones to provide targeted advertising and data harvesting without the consent of users.

216. Defendant monitors, tracks, and logs every browser connection made by users of the subject electronic devices.

217. Defendant assigns each installation of the subject software a unique machine and user identification code.

218. Every time a user attempts to access a website through a browser, the subject programs intercept the connection and re-routes it through a proxy that also sends user information to servers owned or controlled by Defendant.

219. Users of the subject electronic devices do not have a choice in participating in Defendant's business practices.

220. Defendant receives profit for this activity through a commission on purchases made at a merchant or selling data harvested during website users' interaction with the platform.

221. Defendant received substantial profits through the subject programs that Defendant would not have downloaded had Defendant properly disclosed the function and/or flaws in the subject programs.

222. Defendant was conferred a benefit in revenue that it would not have received from Plaintiff for which it should equitably compensate Plaintiff and Class Members. Alternatively stated, Defendant was improperly enriched by its improper conduct and, under principles of equity, is required to compensate Plaintiff and other Class Members for Defendant's unjust enrichment.

223. Defendant further also, received and retained money belonging to Plaintiffs and the Class.

224. Defendant appreciates or has knowledge of such benefit.

225. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members, which Defendant has unjustly received as a result of its unlawful actions.

226. As a result of Defendant's conduct, Plaintiffs and the Class suffered and will continue to suffer actual damages including, but not limited to, the release of their Private Information; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; and, time spent initiating fraud alerts. Plaintiffs and Class members suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, other economic and noneconomic losses.

**COUNT IV. Unfair and Deceptive Business Practices**
**(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)**

227. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs

as if fully set forth herein.

228. Plaintiffs bring this Count individually, and on behalf of all similarly situated residents of each of the 50 States and the District of Columbia, for violations of the respective statutory consumer protection laws, as follows:

a. the Alabama Deceptive Trade Practices Act, Ala. Code 1975, § 8–19–1, *et seq*.

b. the Alaska Unfair Trade Practices and Consumer Protection Act, AS §45.50.471, *et seq*.;

c. the Arizona Consumer Fraud Act, A.R.S §§ 44-1521, *et seq*.;

d. the Arkansas Deceptive Trade Practices Act, Ark. Code §§ 4-88-101, *et seq*.;

e. the California Unfair Competition Law, Bus. & Prof. Code §§17200, *et seq*. and 17500 *et seq*.;

f. the California Consumers Legal Remedies Act, Civil Code §1750, *et seq*.;

g. the Colorado Consumer Protection Act, C.R.S.A. §6-1-101, *et seq*.;

h. the Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110, *et seq*.;

i. the Delaware Consumer Fraud Act, 6 Del. C. § 2513, *et seq*.;

j. the D.C. Consumer Protection Procedures Act, DC Code § 28-3901, *et seq*.;

k. the Florida Deceptive and Unfair Trade Practices Act, FSA § 501.201, *et seq*.;

l. the Georgia Fair Business Practices Act, OCGA § 10-1-390, *et seq*.;

m. the Hawaii Unfair Competition Law, H.R.S. § 480-1, *et seq*.;

n. the Idaho Consumer Protection Act, I.C. § 48-601, *et seq*.;

o. the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1 *et seq*.;

p. the Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, *et seq*.;

q. the Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, *et seq.*;

r. the Kansas Consumer Protection Act, K.S.A. § 50-623, *et seq.*;

s. the Kentucky Consumer Protection Act, KRS 367.110, *et seq.*;

t. the Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, *et seq.*;

u. the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, *et seq.*;

v. the Maryland Consumer Protection Act, MD Code, Commercial Law, §13-301, *et seq.*;

w. the Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, *et seq.*;

x. the Michigan Consumer Protection Act, M.C.L.A. 445.901, *et seq.*;

y. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. §325F.68, *et seq.*;

z. the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq*.

aa. the Missouri Merchandising Practices Act, V.A.M.S. § 407, *et seq.*;

bb. the Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, *et seq.*;

cc. the Nebraska Consumer Protection Act, Neb. Rev. St. §§ 59-1601, *et seq.*;

dd. the Nevada Deceptive Trade Practices Act, N.R.S. 41.600, *et seq.*;

ee. the New Hampshire Regulation of Business Practices for Consumer Protection, N.H. Rev. Stat. § 358-A:1, *et seq.*;

ff. the New Jersey Consumer Fraud Act, N.J.S.A. 56:8, *et seq.*;

gg. the New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, *et seq.*;

hh. the New York Consumer Protection from Deceptive Acts and Practices, N.Y. GBL (McKinney) § 349, *et seq.*;

ii. the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq.*;

jj. the North Dakota Consumer Fraud Act, N.D. Cent. Code Chapter 51-15, *et seq.*;

kk. the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*;

ll. the Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, *et seq.*;

mm. the Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq.*;

nn. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq.*;

oo. the Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1- 5.2(B), *et seq.*;

pp. the South Carolina Unfair Trade Practices Act, SC Code 1976, §§ 39-5-10, *et seq.*;

qq. the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq.*;

rr. the Tennessee Consumer Protection Act, T.C.A. § 47-18-101, *et seq.*;

ss. the Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, *et seq.*;

tt. the Utah Consumer Sales Practices Act, UT ST § 13-11-1, *et seq.*;

uu. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, *et seq.*;

vv. the Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, *et seq.*;

ww. the Washington Consumer Protection Act, RCWA 19.86.010, *et seq.*;

xx. the West Virginia Consumer Credit and Protection Act, W. Va. Code § 46A-1-101, *et seq.*;

yy. the Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100.18, *et seq.*; and

zz. the Wyoming Consumer Protection Act, WY ST § 40-12-101, *et seq*.

229. Defendant violated the statutes set forth (collectively, the "Consumer Protection Acts") above by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs and Class Members' PII, and by allowing third parties to access Plaintiffs' and Class Members' PII.

230. Defendant further violated the Consumer Protection Acts by failing to disclose to the consumers that its data security practices were inadequate, thus inducing consumers to make purchases at Temu.

231. Defendant's acts and/or omissions constitute fraudulent, deceptive, and/or unfair acts or omissions under the Consumer Protection Acts.

232. Plaintiffs and other Class Members were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their PII.

233. Defendant intended for Plaintiffs and other Class Members to rely on Defendant to protect the information furnished to it in connection with debit and credit card transactions and/or otherwise collected by Defendant, in such manner that Plaintiffs' PII would be protected, secure and not susceptible to access from unauthorized third parties.

234. Defendant instead handled Plaintiffs' and other Class Members' information in such manner that it was compromised.

235. Defendant failed to follow industry best practices concerning data security or was negligent in preventing the Data Breach from occurring.

236. It was foreseeable that Defendant's willful indifference or negligent course of conduct

in handling PII it collected would put that information at the risk of compromise by data thieves.

237. On information and belief, Defendant benefited from mishandling the PII of it app users because, by not taking effective measures to secure this information, Defendant saved on the cost of providing data security.

238. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiffs' and Class Members' reliance on Defendant's deception that their Private Information was secure.

239. Defendant's conduct offends public policy and constitutes unfair acts or practices under the Consumer Protection Acts because Defendant caused substantial injury to Class Members that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers.

240. Defendant's acts or practice of failing to employ reasonable and appropriate security measures to protect Private Information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a), which the courts consider when evaluating claims under the Consumer Protection Acts, including 815 ILCS 505/2.

241. Defendant's conduct constitutes unfair acts or practices as defined in the Consumer Protection Acts because Defendant caused substantial injury to Class members, which injury is not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

242. Defendant also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, et. seq., which provides, at Section 10:

Notice of Breach.

> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

243. Plaintiffs and other Class Members have suffered injury in fact and actual damages including lost money and property as a result of Defendant's violations of the Consumer Protection Acts.

244. Defendant's fraudulent and deceptive behavior proximately caused Plaintiffs' and Class Members' injuries, and Defendant conducted itself with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

245. Defendant violated the Consumer Protection Acts, which laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

246. Defendant's failure to disclose information concerning the Data Breach directly and promptly to affected customers, constitutes a separate fraudulent act or practice in violation of the Consumer Protection Acts, including California Business & Professions Code § 17200, *et seq*.

247. The California Plaintiffs seek restitution pursuant to the Consumer Protection Acts, including California Business & Professions Code § 17203, and injunctive relief on behalf of the Class.

248. Plaintiffs seek attorney's fees and damages to the fullest extent permitted under the

Consumer Protection Acts, including N.Y. G.B.L. § 349(h).

**COUNT V.**
**Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*.**
**(on Behalf of the National Class)**

249. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though fully set forth herein.

250. The Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq*., prohibits the interception of any wire, oral, or electronic communications without the consent. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communications is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

251. A "protected computer" under the CFAA includes any computer "which is used in

252. or affecting interstate or foreign commerce or communication." *Id*. § 1030(e)(2). Plaintiff's cellphone device is protected computer used in interstate commerce because it is connected to the internet. *See United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) ("With a connection to the Internet, the … computers were part of a system that is inexorably intertwined with interstate commerce.").

253. "Intercept" is defined as the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

254. "Contents" is defined as "include[ing] any information concerning substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

255. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock

company, trust, or corporation." 18 U.S.C. § 2510(6).

256. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence, or any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…." 18 U.S.C. § 2510(12).

257. Defendant is a "person" for purposes of the Wiretap Act because it is a corporation.

258. Plaintiff's and Class Members' sensitive personal information and data were intercepted by Defendant through "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

259. Plaintiff and Class Members reasonably believed that Defendant was not intercepting, recording, or disclosing the electronic communications.

260. Plaintiff's and Class Members' electronic communications were intercepted during transmission, without consent and for the unlawful and/or wrongful purpose of monetizing private information and data, including by using private information and data to develop marketing and advertising strategies.

261. Defendant's actions were at all relevant times knowing, willful, and intentional, particularly because Defendant is a sophisticated party who knows the type of data it intercepts through its own products. Moreover, experts who uncovered the program injections have explained that the inclusion of the program injections were intentional, non-trivial engineering tasks—the kind that do not happen by mistake or randomly.

262. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by the interception, disclosure and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in

an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made by Defendant as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

263. Plaintiff and the other Class members suffered and will continue to suffer damages including but not limited to loss of their information and loss of money and costs incurred, all of which have ascertainable value to be proven at trial.

**COUNT VI. Violations of the Computer Fraud and Abuse Act, 18 U.S.C § 1030, *et seq*. (on Behalf of the National Class)**

264. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

265. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

266. Defendant violated 18 U.S.C. 1030 by intentionally accessing Plaintiff's and Class Members' computers without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

267. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA.

268. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the

transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

269. Plaintiff's computer is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

270. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of programs downloaded to Plaintiff's computer, which is a protected computer as defined above. By storing sniffing code to access, collect, and transmits details of Plaintiff's web activities and communications, Defendant intentionally caused damage without authorization to those Class Members' computers by impairing the integrity of the computers.

271. Defendant violated 18 U.S.C. 1030(a)(5)(A)(ii) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiff's and Class Members computers by impairing the integrity of data and/or system and/or information.

272. Defendant violated 18 U.S.C. 1030 (a)(5)(A)(iii) by intentionally accessing Plaintiff and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiff and Class Members.

273. Plaintiff and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

274. Plaintiff and Class Members have suffered loss by reason of these violations, as defined

in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

275. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

276. As a result of these takings, Defendant's conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

277. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, the right of privacy.

278. Defendant's unlawful access to Plaintiff's and Class Members' computers and electronic communications has caused Plaintiff and Class Members irreparable injury.

**COUNT VII. Trespass to Personal Property/Chattels**
**(on Behalf of the National Class)**

279. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

280. The common law prohibits the intentional intermeddling with a chattel, including an electronic device, in possession of another that results in the deprivation of the use of the chattel or impairment of the condition, quality, or usefulness of the chattel.

281. Defendant engaged in deception and concealment to gain access to the subject computers.

282. By engaging in the acts described above without the authorization or in excess of consent given by Plaintiff and other Class members, Defendant dispossessed Plaintiff

and Class members from use and/or access to their computers, cellphone and/or online resources. Further, these acts impaired the use, value, and quality of Plaintiff's and Class members' computers and/or cellphones.

283. Defendant's acts constitute an intentional interference with the use and enjoyment of the subject computers and/or cellphones. By the acts described above, Defendant has repeatedly and persistently engaged in trespass to chattels in violation of the common law.

284. Defendant is liable to Plaintiff in an amount to be determined by the enlightened conscious of a jury for all compensatory, exemplary, and other damages proximately caused and/or flowing from Defendant's trespass to chattels.

**COUNT VIII.**
**Violation of Section 349 of New York General Business Law Deceptive Acts and Practices**
**(and Substantially Similar Laws of the Consumer Fraud States)**
**(on Behalf of the Consumer Fraud Multistate Class)**

285. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

286. Defendant's actions alleged herein constitute unlawful, unfair, deceptive, and fraudulent business practices.

287. Defendant's conduct constitutes acts, uses and/or employment by and/or their agents or employees of deception, fraud, unconscionable and unfair commercial practices, false pretenses, false promises, misrepresentations and/or the knowing concealment, suppression, and/or omission of material facts with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of services, and with the subsequent performance of services and transactions, in violation of section 349 of New York's General Business Law.

288. Defendant's acts and omissions were generally directed at the consuming public.

289. The unfair and deceptive trade acts and practices of Defendant have directly, foreseeably, and proximately caused damages and injury to Plaintiff and other members of the Class.

290. Defendant's violations of Section 349 of New York's General Business Law have damaged Plaintiff and other Class Members, and threaten additional injury if the violations continue.

291. Defendant's acts and omissions, including Defendant's misrepresentations, have caused harm to Class Members in that Class Members have suffered the loss of privacy through the exposure of the personal and private information and evasion of privacy controls on their computers.

292. Plaintiff and Class Members have no adequate remedy at law.

293. Plaintiff, on her own behalf, and on behalf of the Class Members, seeks damages, injunctive relief, including an order enjoining Defendant's Section 349 violations alleged herein, and court costs and attorneys' fees, pursuant to NY Gen Bus. Law § 349.

**COUNT IX.**
**Violation Of New York Right To Privacy Statute, N.Y. Civ. Rights Law § 51 (On behalf of New York and Substantially Similar Laws of the Consumer Fraud States)**
**(on Behalf of the Consumer Fraud Multistate Class)**

294. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

295. N.Y. Civ. Rights Law § 51 prohibits the use of a person's name, portrait, picture, or voice for advertising purposes or for the purposes of trade without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal

guardian.

296. Defendant violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—to third parties, including the Chinese Communist Party and foreign government entities. In addition, based on information and belief, Defendant directly benefited from the use of Plaintiffs' content and information.

297. Prior to using the Plaintiffs' content and information, Defendant never obtained consent.

298. Defendant profited from the commercial use of Plaintiffs' information.

299. Plaintiffs did not receive any compensation in return for this use.

300. Under N.Y. Civ. Rights Law § 51, Plaintiffs seek actual damages suffered, plus any profits attributable to Defendant' unauthorized use of Plaintiffs' information not calculated in actual damages. Plaintiffs also reserve the right to equitable relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**COUNT X.**
**Violation of Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA) Chapter 57, *et seq.***

301. Plaintiffs incorporates by reference all preceding paragraphs as if fully set forth herein.

302. WESCA § 5725 entitled "Civil action for unlawful interception, disclosure or use of wire, electronic or oral communication" provides that "any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication."

303. The terms "wire communication" means "any aural transfer made in whole or in part

through the use of facilities for the transmission of communication by wire, cable or other like connection between the point of origin and the point of reception." § 5702.

304. The term "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." *Id*.

305. The term "interception" means "aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device."

306. Defendant is a "person" for purposes of the Wiretap Act because they are corporations.

307. As described above, the code used by the Temu app secretly accesses, texts, keystrokes, emails, voice recordings, and facial biometrics and other content on users' computers and thus constitutes an "intercepting device" that is used to intercept a wire, oral, or electronic communication through electronic means.

308. Plaintiffs' and Class Members' sensitive personal information, data, and interactions with other individuals and websites, including texts, emails, and other communications, that Defendant secretly intercepted through the Temu app are "wire communications" and/or "electronic communications."

309. Plaintiffs and Class Members reasonably believed that Defendant was not intercepting, recording, or disclosing their electronic communications. Defendant' interception of Plaintiffs' and the Class's communications was done in secret.

310. Plaintiffs' and Class Members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing private information and data, including by using their private information

and data to develop marketing and advertising strategies and utilizing user data for other commercial advantage.

311. Defendant's actions were at all relevant times knowing, willful, and intentional, particularly because Defendant is sophisticated party who knows the type of data it intercepts through its own products. Moreover, experts who have examined the Temu app have concluded that the features of the app that allow these covert interceptions are intentional, non-trivial, engineering tasks—the kind that does not happen by mistake or randomly. These experts also concluded that Defendant sought to conceal the features of the Temu app that accomplished the interception of Plaintiffs' and the Class's communications.

312. Plaintiffs nor Class Members consented to Defendant' interception, disclosure, and/or use of their electronic communications. The third parties and/or websites that Plaintiffs and Class Members visited did not know of or consent to Defendant's interception of the communications. Nor could they—Defendant never sought to obtain, nor did it obtain, Plaintiffs', Class Members', or third parties' consent to intercept Temu users' electronic communications with third parties.

313. Pursuant to WESCA § 5725, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the WESCA and are entitled to: (1) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher (2) Punitive damages and (3) A reasonable attorney's fee and other litigation costs reasonably incurred.

**COUNT XI.**
**Violation of the Right to Privacy Under Mass. Gen. Laws Ch. 214 §1B**
**(On Behalf of the Plaintiffs and the Class)**

314. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

315. Mass. Gen. Laws Ch. 214, § 1B provides that "A person shall have a right against unreasonable, substantial or serious interference with his privacy." The statute provides a private cause of action for damages by those whose privacy rights were violated.

316. Plaintiffs and the Class hold, and at all relevant times held, a legally protected privacy interest in their private and personally identifiable data and content – including user/device Identifiers, biometric identifiers and information, and other private information – on their mobile devices and computers.

317. There is a reasonable expectation of privacy concerning Plaintiffs' and the Class's data and content under the circumstances present.

318. As the materials cited above demonstrate, Defendant have engaged in unreasonable, substantial, and serious interference with Plaintiffs and Class Members' privacy rights.

319. The reasonableness of Plaintiffs' and the Class's expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendant's taking of private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from Plaintiffs' and the Class's mobile devices and other social media accounts.

320. Defendant intentionally intruded upon the Plaintiffs' and the Class's solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the Temu App, including all associated code, to surreptitiously obtain, improperly gain

knowledge of, review, and retain the Plaintiffs' and the Class's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information never intended for public consumption.

321. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

322. Defendant's conduct constitutes and, at all relevant times, constituted a serious invasion of privacy, as Defendant either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of – and allow individuals and companies based in China to take and make use of – Plaintiffs' and the Class's private and personally identifiable data. Defendant intentionally invaded Plaintiffs' and the Class's privacy interests by intentionally designing the Temu App, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain their private and personally identifiable data and content. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

323. Defendant further violated Plaintiffs' and the Class's privacy rights by making Plaintiffs' and the Class's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendant's conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of

their conduct. Further, Defendant's conduct targeted Plaintiffs' and the Class's mobile devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain Plaintiffs' and the Class's private and personally identifiable data and information.

324. Plaintiffs and the Class were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

325. Defendant's conduct was a substantial factor in causing the harm suffered by Plaintiffs and the Class.

326. Plaintiffs and the Class seek compensatory and punitive damages as a result of Defendant's actions. Punitive damages are warranted because Defendant's malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Class and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in future misconduct.

327. Plaintiffs and the Class seek injunctive relief to rectify Defendant's actions, including but not limited to requiring Defendant to stop taking more private and personally identifiable data and information of Plaintiffs and the Class from their mobile devices and computers than is reasonably necessary to operate the Temu App; to make clear disclosures; to obtain Plaintiffs' and the Class's consent to the taking of their private and personally identifiable data and information; to stop allowing individuals in China access to Plaintiffs' private and personally identifiable data and information; to stop transferring such information to servers that are accessible from within China; and to recall and destroy Plaintiffs' and the Class's private and personally identifiable data and information already taken in contravention of Plaintiffs' and the Class's right to

privacy.

328. Plaintiffs and the Class seek restitution and disgorgement for Defendant's violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

329. "One who intentionally intrudes, physically or otherwise, upon the solitude 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." Restatement (2nd) of Torts § 652B. 361. The Plaintiffs and the Class have, and at all relevant times had, a reasonable expectation of privacy in their mobile devices and computers. And their private affairs include their past, present and future activity on their mobile devices and computers.

**COUNT XII.**
**Violation Of The Massachusetts Wiretap Act, Mass. Gen. Laws, Ch. 272, § 99**
**(On Behalf of the Plaintiffs and the Class)**

330. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

331. Mass. Gen. Laws, Ch. 272, § 99 provides that "Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were

violated by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest ….” *Id*. § 99.Q.

332. The term "wire communication" means “any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.” *Id.* 99.B.1.

333. The term "interception" means “to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication….” *Id*. 99.B.4.

334. Defendant are each a “person” for purposes of the Wiretap Act because they are corporations.

335. As described above, the code used by the Temu App secretly accesses, texts, emails and other content on users’ computers and thus constitutes an “intercepting device” that is used to intercept a wire, oral, or electronic communication through electronic means.

336. Plaintiffs’ and Class Members’ sensitive personal information, data, and interactions with other individuals and websites, including texts, emails, and other communications, that Defendant secretly intercepted through the Temu App are “wire communications”.

337. Plaintiffs and Class Members reasonably believed that Defendant were not intercepting, recording, or disclosing their electronic communications. Defendant’s interception of Plaintiffs’ and the Class’s communications was done in secret.

338. Plaintiffs' and Class Members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing private information and data, including by using their private information and data to develop marketing and advertising strategies and utilizing user data for other commercial advantage.

339. Defendant were not parties to those communications, which occurred between Plaintiffs and Class Members and third parties or other websites they sought to access or accessed. Defendant used Plaintiffs' and Class Members' electronic communications as part of their business model.

340. Defendant's actions were at all relevant times knowing, willful, and intentional, particularly because Defendant are sophisticated parties who know the type of data they intercept through their own products. Moreover, experts who have examined the Temu App have concluded that the features of the app that allow these covert interceptions are intentional, non-trivial, engineering tasks—the kind that does not happen by mistake or randomly. These experts also concluded that Defendant sought to conceal the features of the Temu App that accomplished the interception of Plaintiffs' and the Class's communications.

341. Neither Plaintiffs nor Class Members consented to Defendant's interception, disclosure, and/or use of their electronic communications. The third parties and/or websites that Plaintiffs and Class Members visited did not know of or consent to Defendant's interception of the communications. Nor could they—Defendant never sought to obtain, nor did it obtain, Plaintiffs', Class Members', or third parties' consent to intercept Temu users' electronic communications with third parties.

342. Pursuant to Mass. Gen. Laws, Ch. 272, § 99.Q, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are each entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendant as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $1,000; (3) punitive damages; and (4) reasonable attorneys' fees and other litigation disbursements reasonably incurred.

**COUNT XIII.**
**Violation Of Illinois's Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*.**
**(On Behalf of the Illinois Plaintiffs and the Illinois Subclass)**

343. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

344. Defendant are violating specific statutory protections governing biometric data contained in the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq*. In 2008, Illinois enacted BIPA to address the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Ses. No. 276. The Illinois Legislature recognized the importance of protecting the privacy of individuals' biometric data, finding that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse [and] is at

heightened risk for identity theft ….” *Id*. 239. As the Illinois Supreme Court has recognized, through BIPA, “our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information.” Rosenbach v. Six Flags Entm’t Corp., 129 N.E.3d 1197, 1206 (Ill. 2019)

345. BIPA thus focuses on “biometric identifiers” and “biometric information.” Biometric identifiers consist of “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10. A “scan” under BIPA means to examine by observation or checking, or systematically in order to obtain data especially for display or storage. In re Facebook Biometric Information Privacy Litigation, 2018 WL 2197546, *3 (N.D. Cal. May 14, 2018). “Geometry” under BIPA is the relative arrangement of parts or elements. Id. Neither the term “scan” nor the term “geometry” requires “actual or express measurements of spatial quantities like distance, depth, or angles.” Id. Biometric information constitutes “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” 740 ILCS 14/10.

346. BIPA makes it unlawful for any private entity to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized representative.”

740 ILCS 14/15(b). At all relevant times, the Illinois Plaintiffs were residents of Illinois and each is a "person" and/or a "customer" within the meaning of BIPA. 740 ILCS 14/15(b).

347. Each Defendant is, and at all relevant times was, a "corporation, limited liability company, association, or other group, however organized," and thus is, and at all relevant times was, a "private entity" under the BIPA. 740 ILCS 14/10.

348. The Illinois Plaintiffs and the Illinois Subclass had their "biometric identifiers," including their "biometric information" collected, captured, received, or otherwise obtained by Defendant as a result of the Illinois Plaintiffs' and the Illinois Subclass's use of the Temu App. 740 ILCS 14/10.

349. At all relevant times, Defendant systematically and surreptitiously collected, captured, received or otherwise obtained the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them or their "legally authorized representatives."

350. In fact, Defendant failed to properly inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other "legally authorized representatives," in writing (or in any other way) that the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" were being "collected or stored" by Defendant. Nor did Defendant inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other "legally authorized representatives," in writing of the specific purpose and length of term for which the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and

"biometric information" were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2)

351. Defendant's unauthorized collection of users' biometric data is particularly harmful here given the access that the Chinese government has to such data. The Chinese government has aggressively sought to collect such data and information in order to further the country's advances in artificial intelligence.

352. As the South China Morning Post reported: "China's goal of becoming a global leader in artificial intelligence (AI) is nowhere more manifested than in how facial recognition technology has become a part of daily life in the world's second-largest economy. Facial recognition systems, which are biometric computer applications that automatically identify an individual from a database of digital images, are now being used extensively in areas such as public security, financial services, transport and retail across the country." 80In fact, the Chinese government employs a variety of biometrics for population surveillance and control: "In addition to voice recognition, there are facial and pupil recognition, gathering of DNA samples—building the world's largest DNA database—and fingerprint scans."[81]

353. BIPA also makes it unlawful for a private entity "in possession of a biometric identifier or biometric information" to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

354. Defendant are, and at all relevant times were, "in possession of" the Illinois Plaintiffs'

[80] https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushingfacial-recognition-technology

[81] https://vlifestyle.org/codec-news/?l=business/content-2254742-china-gathers-people-s-voicesnew-identification-technology-drawing-concerns.

and the Illinois Subclass's "biometric identifiers," including but not limited to their "biometric information." Defendant profited from such "biometric identifiers" and "biometric information" by using them for targeted advertising and the generation of increased demand for and use of Defendant's other products. 740 ILCS 14/15(c).

355. Finally, BIPA prohibits private entities "in possession of a biometric identifier or biometric information" from "disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person's or a customer's biometric identifier or biometric information unless" any one of four enumerated conditions are met. 740 ILCS 14/15(d)(1)-(4). None of such conditions are met here.

356. Defendant disclose, redisclose and disseminate, and at all relevant times disclosed, redisclosed and disseminated, the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers," including but not limited to their "biometric information" without the consent of any of them or their "legally authorized representatives." 740 ILCS 14/15(d)(1). Moreover, the disclosures and redisclosures did not "complete[] a financial transaction requested or authorized by" the Illinois Plaintiffs, the Illinois Subclass or any of their legally authorized representatives. 740 ILCS 14/15(d)(2). Nor are, or at any relevant times were, the disclosures and redisclosures "required by State or federal law or municipal ordinance." 740 ILCS 14/15(d)(3). Finally, at no point in time were the disclosures ever "required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d)(4). BIPA mandates that a private entity "in possession of biometric identifiers or biometric information" "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric

information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). But Defendant do not publicly provide any written policy establishing any retention schedule or guidelines for permanently destroying the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information." 740 ILCS 14/15(a).

357. BIPA also commands private entities "in possession of a biometric identifier or biometric information" to: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits and protects other confidential and sensitive information. 740 ILCS 14/15(e). Based on the facts alleged herein, including Defendant's lack of an adequate public written policy, their failure to inform Temu users that Defendant obtain such users' "biometric identifiers" and "biometric information," their failure to obtain written consent to collect or otherwise obtain Temu users' "biometric identifiers" and "biometric information," and their unauthorized dissemination of Temu users' "biometric identifiers" and "biometric information," Defendant have violated this provision too.

358. Defendant recklessly or intentionally violated each of BIPA's requirements and infringed the Illinois Plaintiffs' and the Illinois Subclass's rights to keep their immutable and uniquely identifying biometric identifiers and biometric information private. As individuals subjected to each of Defendant's BIPA violations above, the

Illinois Plaintiffs and the Illinois Subclass are and have been aggrieved. 740 ILCS 14/20.

359. On behalf of themselves and the Illinois Subclass, the Illinois Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of the Illinois Plaintiffs and the Illinois Subclass by requiring Defendant to comply with BIPA's requirements; (2) $1,000.00 or actual damages, whichever is greater, for each negligent violation of BIPA by Defendant; (3) $5,000.00 or actual damages, whichever is greater, for each intentional or reckless violation of BIPA by Defendant; and (4) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses. 740 ILCS 14/20(1)-(4)

**COUNT XIV.**
**Invasion of Privacy - Intrusion, Public Disclosure of Private Facts, Misappropriation of Likeness and Identity, and California Constitutional Right to Privacy**
(*On Behalf of Plaintiff Batalas and All Other Similarly Situated California Consumers*)

360. The California Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

361. The California Plaintiffs had a reasonable expectation of privacy in the Private Information Defendant mishandled.

362. By failing to keep the California Plaintiffs' Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded California Plaintiffs' privacy by:

a. Intruding into California Plaintiffs' private affairs in a manner that would be highly offensive to a reasonable person;

b. Publicizing private facts about the California Plaintiffs, which is highly offensive to a reasonable person;

c. Using and appropriating California Plaintiffs' identity without their consent; and

d. Violating California Plaintiffs' right to privacy under California Constitution, Article 1, Section 1, through the improper use of their Private Information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

363. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in California Plaintiffs' position would consider Defendant's actions highly offensive.

364. Defendant invaded California Plaintiffs' right to privacy and intruded into California Plaintiffs' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

365. As a proximate result of such misuse and disclosures, California Plaintiffs' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of California Plaintiffs' protected privacy interests.

366. In failing to protect California Plaintiffs' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of California Plaintiffs and the Class Members' rights to have such information kept confidential and private. The California Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of themselves and the Class.

**COUNT XV.**
**Violation of State Data Breach Acts**
**(On Behalf of Plaintiffs and All Other Similarly Situated United States Consumers)**

367. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

368. Defendant owns, licenses and/or maintains computerized data that includes Plaintiffs' and Class Members' PII.

369. Defendant was required to, but failed, to take all reasonable steps to dispose, or arrange for the disposal, of records within its custody or control containing personal information when the records were no longer to be retained, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

370. Defendant's conduct, as alleged above, violated the data breach statutes of many states, including:

a. California, Cal. Civ. Code §§ 1798.80 et. seq.;

b. Hawaii, Haw. Rev. Stat. § 487N-1–4 (2006);

c. Illinois, 815 Ill. Comp Stat. Ann. 530/1–/30 (2006);

d. Louisiana, La. Rev. Stat. § 51:3071-3077 (2005), and L.A.C. 16: III.701;

e. Michigan, Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006);

f. New Hampshire, N.H. Rev. Stat. Ann. §§ 359-C:19–C:21, 358-A:4 (2006)., 332-I:1–I:610;

g. New Jersey, N.J. Stat. Ann. § 56:8-163–66 (2005);

h. North Carolina, N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009);

i. Oregon, Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624 (2011);

j. Puerto Rico, 10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008);

k. South Carolina, S.C. Code § 1-11-490 (2008); S.C. Code § 39-1-90 (2009);

l. Virgin Islands, 14 V.I.C. § 2208, *et seq*. (2005);

m. Virginia, Va. Code Ann. § 18.2-186.6 (2008); Va. Code Ann. § 32.1– 127.1:05 (2011); and

n. the District of Columbia, D.C. Code § 28-3851 to 28-3853 (2007) (collectively, the "State Data Breach Acts").

371. Defendant was required to, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

372. The Data Breach constituted a "breach of the security system" within the meaning of section 1798.82(g) of the California Civil Code, and other State Data Breach Acts.

373. The information compromised in the Data Breach constituted "personal information" within the meaning of section 1798.80(e) of the California Civil Code, and other State Data Breach Acts.

374. Like other State Data Breach Acts, California Civil Code § 1798.80(e) requires disclosure of data breaches "in the most expedient time possible and without unreasonable delay . . . ."

375. Defendant violated Cal. Civ. Code § 1798.80(e) and other State Data Breach Acts by unreasonably delaying disclosure of the Data Breach to Plaintiffs and other Class Members, whose PII was, or was reasonably believed to have been, acquired by an unauthorized person.

376. Upon information and belief, no law enforcement agency instructed Defendant that

notification to Plaintiffs and Class Members would impede a criminal investigation.

377. As a result of Defendant's violation of State Data Breach Acts, including Cal. Civ. Code § 1798.80, *et seq.*, Plaintiffs and Class Members incurred economic damages, including expenses associated with monitoring their personal and financial information to prevent further fraud.

378. Plaintiffs, individually and on behalf of the Class, seek all remedies available under Cal. Civ. Code § 1798.84 and under the other State Data Breach Acts, including, but not limited to: (a) actual damages suffered by Class Members as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or reckless violation of Cal. Civ. Code §1798.83. (c) equitable relief; and (d) reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

379. Because Defendant was guilty of oppression, fraud or malice, in that it failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights, Plaintiffs also seek punitive damages, individually and on behalf of the Class.

**COUNT XVI.**
**Violation of The California Comprehensive Data Access and Fraud Act, CAL. PEN. C. § 502**
(On Behalf of the California Plaintiffs and California Subclass)

380. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

381. Defendant's acts violate Cal. Pen. C. § 502(c)(1) because they have knowingly accessed, and continue to knowingly access, data and computers to wrongfully control or obtain data. The Plaintiffs' and the Subclass's private and personally identifiable data and content accessed by Defendant – including user/device identifiers, biometric identifiers and information, and other private data – far exceeds any reasonable use of

the Plaintiffs' and the Subclass's data and content to operate the Temu app. There is no justification for Defendant's surreptitious collection and transfer of the Plaintiffs' and the Subclass's private and personally identifiable data and content from their devices and computers and allowing access to that information to individuals and third-party companies in China that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

382. Defendant's acts violate Cal. Pen. C. § 502(c)(2) because they have knowingly accessed and without permission taken, copied, and made use of data from a computer – and they continue to do so. Defendant did not obtain permission to take, copy, and make use of the Plaintiffs' and the Subclass's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from their devices – and provide access to individuals and companies that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

383. Accordingly, the Plaintiffs and the Subclass are entitled to compensatory damages, including "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access," injunctive relief, and attorneys' fees. Cal. Pen. C. § 502(e)(1), (2).

**COUNT XVII.**
**Violation of The Right of Privacy Under the California Constitution**
**(On Behalf of the California Plaintiffs and California Subclass)**

384. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

385. Plaintiffs and the California Subclass hold, and at all relevant times held, a legally protected privacy interest in their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data – on their devices and computers.

386. There is a reasonable expectation of privacy concerning Plaintiffs' and the Subclass's data and content under the circumstances present.

387. The reasonableness of Plaintiffs' and the Subclass's expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendant's accessing private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from Plaintiffs' and the Subclass's devices and computers.

388. Defendant's conduct constitutes and, at all relevant times, constituted a serious invasion of privacy, as Defendant either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of – and allow individuals and companies based in China to take and make use of – Plaintiffs' and the Subclass's private and personally identifiable data and content. Defendant intentionally invaded Plaintiffs' and the Subclass's privacy interests by intentionally designing the Temu app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain their private and personally identifiable data and content. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendant's intrusion is heightened by Defendant's making Plaintiffs' and the

Subclass's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendant's conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendant's conduct targeted Plaintiffs' and the Subclass's devices, which contain Plaintiffs' and the Subclass's private and personally identifiable data and content.

389. Plaintiffs and the Subclass were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

390. Defendant's conduct was a substantial factor in causing the harm suffered by Plaintiffs and the Subclass.

391. Plaintiffs and the Subclass seek compensatory and punitive damages as a result of Defendant's actions. Punitive damages are warranted because Defendant's malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Subclass and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in future misconduct.

392. Plaintiffs and the Subclass seek injunctive relief to rectify Defendant's actions, including but not limited to requiring Defendant (a) to stop taking more private and personally identifiable data and content of Plaintiffs and the Subclass from their devices and computers than is reasonably necessary to operate the Temu app; (b) to make clear disclosures of Plaintiffs' and the Subclass's private and personally identifiable data and content that is reasonably necessary to operate the Temu app; (c) to obtain Plaintiffs' and the Subclass's consent to the taking of their private and personally identifiable data

and content; (d) to stop providing access to the Plaintiffs' private and personally identifiable data and content to individuals in China or transferring such data to servers or companies whose data is accessible from within China; and (e) to recall and destroy Plaintiffs' and the Subclass's private and personally identifiable data and content already taken in contravention of Plaintiffs' and the Subclass's right to privacy under the California Constitution.

393. The Plaintiffs and the Subclass seek restitution and disgorgement for Defendant's violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44

**COUNT XVIII.**
**Intrusion Upon Seclusion**
(On Behalf of the California Plaintiffs and California Subclass)

394. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

395. Defendant's acts violate Cal. Pen. C. § 502(c)(1) because they have knowingly accessed, and continue to knowingly access, data and computers to wrongfully control or obtain data. The Plaintiffs' and the Subclass's private and personally identifiable data and content accessed by Defendant – including user/device identifiers, biometric identifiers and information, and other private data – far exceeds any reasonable use of

the Plaintiffs' and the Subclass's data and content to operate the Temu app. There is no justification for Defendant's surreptitious collection and transfer of the Plaintiffs' and the Subclass's private and personally identifiable data and content from their devices and computers and allowing access to that information to individuals and third-party companies in China that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

396. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

397. "One who intentionally intrudes, physically or otherwise, upon the solitude 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." Restatement (2nd) of Torts § 652B.

398. The Plaintiffs and the California Subclass have, and at all relevant times had, a reasonable expectation of privacy in their devices and computers, and their private affairs include their past, present and future activity on their devices and their other media accounts.

399. The reasonableness of the Plaintiffs' and the Subclass's expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendant's taking of private and personally identifiable data and content from the Plaintiffs' and the Subclass's devices and computers.

400. Defendant intentionally intruded upon the Plaintiffs' and the Subclass's solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the Temu app, including all associated code, to surreptitiously obtain, improperly gain

knowledge of, review, and retain the Plaintiffs' and the Subclass's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information.

401. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendant's intrusion is heightened by Defendant's making the Plaintiffs' and the Subclass's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendant's conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendant's conduct targeted the Plaintiffs' and the Subclass's devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain the Plaintiffs' and the Subclass's private and personally identifiable data and content.

402. The Plaintiffs and the Subclass were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

403. Defendant's conduct was a substantial factor in causing the harm suffered by the Plaintiffs and the Subclass.

404. The Plaintiffs and the Subclass seek nominal and punitive damages as a result of Defendant's actions. Punitive damages are warranted because Defendant's malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Subclass, and were made in conscious disregard of their rights. Punitive damages are also

warranted to deter Defendant from engaging in future misconduct.

405. The Plaintiffs and the Subclass seek injunctive relief to rectify Defendant's actions, including but not limited to requiring Defendant (a) to stop taking more private and personally identifiable data and content from the Plaintiffs' and the Subclass's devices and computers accounts than is reasonably necessary to operate the Temu app; (b) to make clear disclosures of the Plaintiffs' and the Subclass's private and personally identifiable data and content that is reasonably necessary to operate the Temu app; (c) to obtain the Plaintiffs' and the Subclass's consent to the taking of such private and personally identifiable data and content; (d) to stop providing access to the Plaintiffs' and the Subclass's private and personally identifiable data and content to individuals in China or transferring such data to servers or companies whose data is accessible from within China; and (e) to recall and destroy the Plaintiffs' and the Subclass's private and personally identifiable data and content already taken in contravention of the Plaintiffs' and the Subclass's privacy rights.

406. Plaintiffs and the Subclass seek restitution and disgorgement for Defendant's intrusion upon seclusion. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

**COUNT XIX.**
**Violation of the California Unfair Competition Law, BUS. & PROF. C. §§ 17200 *et seq*.**
**(On Behalf of the California Plaintiffs and California Subclass)**

407. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

408. The Unfair Competition Law, California Business & Professions Code §§ 17200, *et seq*. (the "UCL"), prohibits any "unlawful," "unfair," or "fraudulent" business act or practice, which can include false or misleading advertising.

409. Defendant violated, and continue to violate, the "unlawful" prong of the UCL through violation of statutes, constitutional provisions, and common law, as alleged herein.

410. Defendant violated, and continue to violate, the "unfair" prong of the UCL because they accessed private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from the Plaintiffs' and the Subclass's devices and computers under circumstances in which the Plaintiffs and the Subclass would have no reason to know that such data and content was being taken.

411. Plaintiffs and the Subclass had no reason to know because (i) there was no disclosure, or no effective disclosure, of Defendant's collection and transfer of the Plaintiffs' and the Subclass's biometric identifiers and information, and private data and information; (ii) there was no disclosure that Defendant had embedded source code within the Temu app that makes Plaintiffs' and the Subclass's private and personally identifiable data and content accessible to third-party companies and individuals based in China where such companies and individuals are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (iii) there was no effective

disclosure of the wide range of private and personally identifiable data and content that Defendant took from the Plaintiffs' and the Subclass's devices. Defendant violated, and continue to violate, the "fraudulent" prong of the UCL because (i) Defendant made it appear that the Plaintiffs' private and personally identifiable data and content would not be collected and transferred unless the Plaintiffs and the Subclass chose to do so, but in fact Defendant collected and transferred such data and content without notice or consent; (ii) Defendant made it appear that the Plaintiffs' and the Subclass's private and personally identifiable data and content would not be provided to individuals or companies that are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (iii) Defendant have intentionally refrained from disclosing the uses to which the Plaintiffs' and the Subclass's private and personally identifiable data and content has been put, while simultaneously providing misleading reassurances about Defendant's data collection and use practices. The Plaintiffs and the Subclass were misled by Defendant's concealment, and had no reason to believe that Defendant had taken the private and personally identifiable data and content that they had taken or used it in the manner they did.

412. In addition, Defendant fail to adequately disclose that users' data will be accessible to individuals in China, and ultimately accessible by the Chinese communist government. To the contrary, Defendant assured Plaintiffs and the Subclass of the privacy of their data, while under Chinese law the Chinese government has an absolute right to access users' data.

413. Defendant's conduct is particularly egregious because these violations extend to minor users whom Defendant acknowledge should not be using the platform. Indeed, through

their promotion through various influencers and other means, Defendant have encouraged minor use. Moreover, they have failed to incorporate appropriate age verification and other measures in the Temu app necessary to prevent underage use and have incorporated features in the design of the Temu app that actually facilitate underage use.

414. In addition, Defendant have utilized a variety of deceptive, unfair and manipulative means to increase usage of the Temu app and, in turn, the collection of user data.

415. Plaintiffs and the Subclass have been harmed and have suffered economic injury as a result of Defendant's UCL violations. First, Plaintiffs and the Subclass have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendant's covert theft of their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information.

416. Defendant, as a result of their conduct, have been able to reap unjust profits and revenues in violation of the UCL. This includes Defendant's profits and revenues from their targeted advertising, revenues from the sale of goods on the Temu site, and the increased consumer demand for and use of Defendant's products. Plaintiffs and the Subclass seek restitution and disgorgement of these unjust profits and revenues.

417. Unless restrained and enjoined, Defendant will continue to misrepresent their private and personally identifiable data and content collection and use practices, and will not recall and destroy Plaintiffs' and the Subclass's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

**COUNT XX.**
**Violation of the California False Advertising Law, BUS. & PROF. C. §§ 17500 *et seq*.**
(On Behalf of the California Plaintiffs and California Subclass)

418. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

419. California's False Advertising Law (the "FAL") – Cal. Bus. & Prof. Code §§ 17500, *et seq*. – prohibits "any statement" that is "untrue or misleading" and made "with the intent directly or indirectly to dispose of" property or services.

420. Defendant's advertising is, and at all relevant times was, highly misleading.

421. Defendant do not disclose at all, or do not meaningfully disclose, the private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private data and information – that they have collected and transferred from the Plaintiffs' and the Subclass's devices and computers. Nor do Defendant disclose that the Plaintiffs' and the Subclass's private and personally identifiable data and content have been made available to foreign government entities.

422. Reasonable consumers, like the Plaintiffs and the Subclass, are – and at all relevant times were – likely to be misled by Defendant's misrepresentations. Reasonable consumers lack the means to verify Defendant's representations concerning their data and content collection and use practices, or to understand the fact or significance of Defendant's data and content collection and use practices.

423. Plaintiffs and the Subclass have been harmed and have suffered economic injury as a result of Defendant's misrepresentations. First, they have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendant's accessing their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information.

424. Defendant, as a result of their misrepresentations, have been able to reap unjust profits and revenues. This includes Defendant's profits and revenues from their targeted advertising, revenue from the sale of goods on the Temu site, and increased consumer demand for and use of Defendant's other products and services. Plaintiffs and the Subclass seek restitution and disgorgement of these unjust profits and revenues.

425. Unless restrained and enjoined, Defendant will continue to misrepresent their private and personally identifiable data and content collection and use practices and will not recall and destroy Plaintiffs' and the Subclass's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

**COUNT XXI.**
**Texas Deceptive Trade Practices and Consumer Protection Act**
**Tex. Bus. & Com. C. § 17.50(a) *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Texas Subclass)**

426. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

427. Plaintiffs bring this claim individually and on behalf of the Texas Subclass.

428. Plaintiff James Lafata is a consumer under the meaning of the Deceptive Trade Practice and Consumer Protection Act (hereinafter "DTPCA").

429. As specifically enumerated in subdivision of Subsection (b) of Section 17.46 of the subchapter of the DTPCA, Defendant have failed to disclose information concerning the Temu app known at the time of the purchases made by the Texas subclass pertaining to its data insecurities and data harvesting.

430. The failure to disclose was used to induce the Texas Subclass into transactions that they otherwise would not have entered had the information be disclosed.

431. As stated above, Plaintiff James Lafata can show that subsequent to the installation of the defendant's application on Plaintiff James Lafata's device, he encountered unauthorized access to both his Microsoft email account and his bank accounts. Plaintiff James also experienced several unauthorized transactions on his Bank Accounts and Cash App. A report from the Microsoft team corroborated these findings, indicating that Plaintiff James Lafata's email had been compromised. Due to changes made to his security questions by the intruders, the Microsoft team deemed it necessary to permanently suspend his account to prevent further unauthorized activity.

432. Plaintiffs seek to recover up to three times the amount of the economic damages, in addition to damages for mental anguish.

433. Plaintiffs additionally seek court courts and reasonable and necessary attorney fees under the DTPA.

**COUNT XXII.**
**Violations of the Texas Harmful Access by Computer Act, Tex. Penal Code § 33 *et seq*.**
**(on Behalf of the Texas Class)**

434. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

435. Plaintiffs bring this claim individually and on behalf of the Texas Subclass.

436. The Texas Harmful Access by Computer Act ("Texas HACA") creates a civil cause of action for a "person who is injured or whose property has been injured" by knowing or intentional violations of the Texas Penal Code Chapter 33, Computer Crimes.

437. The elements of a plaintiff's claim under the BCS are "(1) an individual knowingly and intentionally accessed their computer, computer network, or computer system; (2) the individual did not have the effective consent of the owner to do so; and, (3) the owner suffered damages as a result.

438. The Texas Court has interpreted a cellphone to qualify as a computer under the Texas Penal Code § 33.01(4).

439. The Texas Court has also interpreted the retrieval of the phone's logs and text messages as access of the phone within Chapter 33's meaning.

440. The injured party is entitled to actual damages and reasonable attorneys' fees and costs.[18] Texas Penal Code Chapter 33, states broadly that whereby [a] person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

441. "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.[20]

442. As mentioned earlier, subsequent to the installation of the defendant's application on Plaintiff James Lafata's device, he encountered unauthorized access to both his Microsoft email account and his bank accounts. Plaintiff James also experienced several unauthorized transactions on his Bank Accounts and Cash App. A report from the Microsoft team corroborated these findings, indicating that Plaintiff James Lafata's email had been compromised. Due to changes made to his security questions by the intruders, the Microsoft team deemed it necessary to permanently suspend his account to prevent further unauthorized activity.

**COUNT XXIII.**
**Violation of Oregon Unlawful Trade Practices Act**
**ORS § 646.638 *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Oregon Subclass)**

443. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

444. Plaintiffs bring this claim individually and on behalf of the Oregon Subclass.

445. "Any person who suffers any ascertainable loss of money or property, real or personal, as a result of willful use or employment by another person of a method, act or practice declared unlawful by ORS 646.608 or 646.648, may bring an individual action in an appropriate court to recover actual damages or $200, whichever is greater. The Court or the jury, as the case may be, may award punitive damages and the court may provide such equitable relief as it deems necessary or proper." ORS 646.638(1).

446. Plaintiff Daniel David Kattan, was a victim of Defendant's unlawful Trade Practices. Plaintiff Daniel David Kattan had made a purchase for AA batteries with Charger from Defendant's website. However, after purchase of the product, Plaintiff only received the batteries and and not the charger.

447. In accordance to 646.638(2), Plaintiffs have served a copy of the Complaint to the Oregon State Attorney General.

**COUNT XXIV.**
**Violation of Georgia Fair Business Practices Act**
**O.C.G.A. § 10-1-399(a) *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Georgia Subclass)**

448. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

449. Plaintiffs bring this claim individually and on behalf of the Georgia Subclass.

450. As set forth above, Defendant have engaged in consumer transactions and consumer acts or practices in the conduct of trade or commerce within the State of Georgia as defined in Georgia Code 10-1-392(a)(7), (10), and (28).

451. The GFBPA proscribes "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce are declared unlawful." O.C.G.A. § 10-1-393(a).

452. To establish a cause of action under the GFBPA, a plaintiff must satisfy the following elements: (1) violation of the Act; (2) causation; and (3) injury.

453. The GFBPA "differs from common law fraud in that it eliminates two of the five required elements of fraud: scienter and intent to deceive."

454. As previously mentioned, Tracy Evette Starling, the plaintiff, can substantiate through her bank statements that several unauthorized charges appeared on her bank cards, leading to the closure of her bank accounts. Despite assurances from the defendant regarding the protection of personal information, this assurance was misleading, as evidenced by numerous instances of unauthorized bank charges reported by Plaintiff and various individuals on the BBB website. Despite being aware of these incidents,

the defendant neglected to enact adequate measures to safeguard the data of the application users. Had the plaintiff been aware of this prior to installing the application, she would have refrained from using the Temu Application nor participate in any transactions associate with Temu.

455. Plaintiffs seek damages on behalf of themselves and the Georgia Subclass in the amount of actual damages suffered.

456. O.C.G.A. § 10-1-399(b) expressly provides that "[t]he demand requirements of this subsection shall not apply if the prospective respondent does not maintain a place of business or does not keep assets within the state.

**COUNT XXV.**
**Violation of New Jersey Fair Business Practices Act**
**N.J. Stat. § 56:8-12 *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated New Jersey Subclass)**

457. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

458. Plaintiffs bring this claim individually and on behalf of the New Jersey Subclass.

459. N.J. Stat. Ann. § 56:8-2.12 provides for a private right of action, to recover monies lost as a result of unconscionable commercial practices, and N.J. Stat. Ann. § 56:8-2.13 states that the rights protected under the Act are cumulative of other rights and remedies under New Jersey law.

460. Defendant' collection and sharing of sensitive data without consumers' consent has caused or is likely to cause substantial injury to consumers or households across Temu's cellphone and computer modalities. Defendant utilized this data to track and target advertising to individual consumers across devices. Defendant engaged in these practices through a medium that consumers would not expect to be used for tracking,

without the consumer's consent.

461. Defendant' collection and sharing of sensitive data without consumer's consent has caused or is likely to cause substantial injury to consumers that is not outweighed by the countervailing benefits to consumers or competition and is not reasonably avoidable by the consumers themselves.

462. This is an unfair act or practice. Each instance of Defendant's unfair tracking constitutes a separate violation under the Fair Business Practices Act.

463. In addition, Defendant's failed to disclose that its Temu app comprehensively collected and shared consumers' app activity from cellphones and computers.

464. Defendant's failure to disclose adequately the material information described in light of the representation set forth, is a deceptive act or practice in violation.

465. Here, actual damage can be ascribed because…

466. Plaintiffs seek treble damages for refunds, pursuant to N.J. Stat. § 56:8-2.11 and 56:8-2.12 and treble damages for violations pursuant to N.J. Stat. § 56:8-19.

**COUNT XXVI.**
**Action for Computer-Related Offenses**
**Conn. Gen. Stat. § 52-570b *et seq.*]**
**(On Behalf of Plaintiffs and All Other Similarly Situated Connecticut Subclass**

467. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

468. Plaintiffs bring this claim individually and on behalf of the Connecticut Subclass.

469. Sec. 52-570b. Action for computer-related offenses.: Conn. Gen. Stat. § 52-570b allows for civil actions against violations of Conn. Gen. Stat. § 53a-251 related to computer offenses and misuse of private personal data.

470. Defendant, knowingly accessed Plaintiff's and Class members without seeking prior

authorization from the users, by accessing their personal computers without authorization.

471. The aforesaid conduct of Defendant is a violation of C.G.S. § 53a-251(a).

472. Plaintiff YO-YO CHEN is an aggrieved person due to Defendant's violation of section 53a-251.

473. Defendant breached the privacy provision by surreptitiously and unlawfully recording the screen and location data of the Temu customers.

474. Upon information and belief, Defendant further misused Plaintiff's computer system information by accessing the computer system and knowingly received or retained data that was disclosed on or copied from Plaintiff's computer.

475. Plaintiff seeks an order directing restitution to himself/ herself and the Connecticut Subclass, in addition to actual damages and damages for unjust enrichment not taken into account in computing damages for actual loss, and treble damages for Defendant's malicious conduct.

**COUNT XXVII.**
**Violation of Michigan Consumer Protection Act**
**MCL § 445.903(1) *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Michigan Subclass)**

476. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

477. Plaintiffs bring this claim individually pursuant to Section 11 of the MCPA, MCL 445.911(1)–(3) and alternatively on behalf of the Michigan Subclass pursuant to Section 11 of the MCPA, MCL 445.911(4).

478. Section 3 of the MCPA, MCL 445.903(1) defines certain unfair, unconscionable, or

deceptive methods, acts, or practices in the conduct of trade or commerce that are unlawful, including but not limited to the following:

A. (s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer.

B. (bb) Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is.

C. (cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

479. Defendant represented to consumers that it protects the personal information of Michigan residents, either implicitly by collecting such personal information or explicitly.

480. Contrary to these representations, intruders were able to gain access to personal information on Defendant's network and the Defendant suffered a data breach. Such representations were likely to mislead consumers acting reasonably under the circumstances into believing that personal information was safeguarded from misuse by third parties and were material to their decisions about whether to entrust the Defendant with personal information, including credit card information.

481. Defendant represented on its website that it accepted payments by credit card thus implicitly represented that it was compliant with the Payment Card Industry Data Security Standard ("PCI DSS"), which is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information

maintain a secure environment to safeguard such information throughout the transaction process.

482. Contrary to these representations the Defendant was not in compliance with the Payment Card Industry Data Security Standard.

483. Defendant, in the course of conducting its business, failed to implement and maintain reasonable security procedures and practices appropriate to protect the personal information of Michigan residents that Defendant owned, licensed, or maintained, and thus did not protect that personal information from unauthorized access, use, destruction, modification, or disclosure.

484. The Defendant's misleading statements to consumers regarding its data protection practices have had the capacity, tendency, or effect of deceiving or misleading consumers and constitute unfair or deceptive trade practices as defined in MCL 445.903(1)(bb).

485. Defendant's failure to adequately inform consumers regarding its data protection practices constitutes a failure to state material facts, the omission of which has deceived or tended to deceive consumers, as set forth above, and constitute unfair or deceptive trade practices as defined in MCL 445.903(1)(s), MCL 445.903(1)(cc).

486. The exemption under MCL does not apply because Defendant does not engage in "transaction specifically authorized by law" and is not regulated by Michigan's Occupational Code.

487. Defendant engaged in the acts and practices alleged herein when it knew or should have known that its conduct was unfair or deceptive, in violation of MCL 445.903(1).

**COUNT XXVIII.**
**Violation of Washington Consumer Protection Act**
**RCW § 19.86.020 *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Washington Subclass)**

488. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

489. Plaintiffs bring this claim individually and on behalf of the Washington Subclass pursuant to Washington Consumer Protection Act ("WCPA"), RCW 19.86.020.

490. Section 20 of the WCPA prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." RCW 19.86.020.

491. Defendant represented to consumers that it protects the personal information of Washington residents, either implicitly by collecting such personal information or explicitly.

492. Contrary to these representations, intruders were able to gain access to personal information on Defendant's network and the Defendant suffered a data breach. Such representations were likely to mislead consumers acting reasonably under the circumstances into believing that personal information was safeguarded from misuse by third parties and were material to their decisions about whether to entrust the Defendant with personal information, including credit card information.

493. Defendant represented on its website that it accepted payments by credit card thus implicitly represented that it was compliant with the Payment Card Industry Data Security Standard ("PCI DSS"), which is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment to safeguard such information throughout the transaction process.

494. Contrary to these representations the Defendant was not in compliance with the Payment Card Industry Data Security Standard.

495. Defendant, in the course of conducting its business, failed to implement and maintain reasonable security procedures and practices appropriate to protect the personal information of Washington residents that Defendant owned, licensed, or maintained, and thus did not protect that personal information from unauthorized access, use, destruction, modification, or disclosure.

496. Additionally, Defendant embedded a code in their application without the app users consent and collected and unlawfully shared consumer health data in violation of RCW 19.373.030 by

497. Additionally, Defendant collected and unlawfully shared consumer biometric identifiers in violation of RCW 19.375.020 by sharing it with third parties and transferring the app users personal information outside of the United States.

498. Defendant engaged in the acts and practices alleged herein which are injurious to the public interest under RCW 19.86.093(2) by virtue of: failing to comply with 19.255 by notifying users of security breaches; and failing to comply with 19.215 by disposing of users' personal information.

499. Defendant engaged in the acts and practices alleged herein which are injurious to the public interest under RCW 19.86.093(3), including by application of RCW 19.373.090 and RCW 19.375.030.

**COUNT XXIX.**
**Violation of Washington Disposal of Personal Information Act**
**RCW § 19.215.020 *et se***
**(On Behalf of Plaintiffs and All Other Similarly Situated Washington Subclass)**

500. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs

as if fully set forth herein.

501. Plaintiffs bring this claim individually and on behalf of the Washington Subclass pursuant to Washington Disposal of Personal Information Act ("WDPIA"), RCW 19.215.020.

502. Section 20 of the WCPA provides that "[a]n entity must take all reasonable steps to destroy, or arrange for the destruction of, personal financial and health information and personal identification numbers issued by government entities in an individual's records within its custody or control when the entity is disposing of records that it will no longer retain." 19.215.020(a).

503. Defendant represented to consumers that it protects the personal information of Washington residents, either implicitly by collecting such personal information or explicitly, including by destroying or arranging for the destruction of, personal financial and health information and personal identification numbers issued by government entities in an individual's records within its custody or control when the entity is disposing of records that it will no longer retain.

504. Contrary to these representations, Defendant willfully shared Washington residents' personal financial and health information and personal identification numbers issued by government with third parties, including the government of the People's Republic of China, which is prohibited by law.

505. Defendant's conduct is not protected by the exemption under RCW 19.215.020(3).

506. Defendant is liable to Plaintiff(s) and the members of the Washington Subclass for damages under RCW 19.215.020(4)(b).

**COUNT XXX.**
**Violation of Washington Notice of Security Breaches Act**
**RCW § 19.255.010 *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Washington Subclass)**

507. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

508. Plaintiffs bring this claim individually and on behalf of the Washington Subclass pursuant to Section 40 of the Washington Notice of Security Breaches Act ("WNSBA"), RCW 19.255.040.

509. Section 10 of the WNSBA, RCW 19.255.010 provides that "[a]ny person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person." RCW 19.255.010(1).

510. It further provides that "[a]ny person or business that maintains or possesses data that may include personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

511. Defendant represented to consumers that it protects the personal information of Washington residents, either implicitly by collecting such personal information or explicitly.

512. Contrary to these representations, intruders were able to gain access to personal information on Defendant's network and the Defendant suffered a data breach.

513. Defendant failed to adequately inform consumers regarding its data breach.

514. Defendant is liable to Washington Plaintiff(s) and the Washington Subclass under Section 40 of the WNSBA. RCW 19.255.040(3)(a).

**COUNT XXXI.**
**Violation of Ohio Consumer Sales Practices Act**
**ORC § 1345.02 *et seq.***
**(On Behalf of Plaintiffs and All Other Similarly Situated Ohio Subclass)**

515. Plaintiffs incorporate the substantive allegations contained in all previous paragraphs as if fully set forth herein.

516. Plaintiffs bring this claim individually and on behalf of the Ohio Subclass pursuant to Section 9 of the Ohio Consumer Sales Practices Act ("OCSPA"), ORC 1345.09.

517. Section 2 of the OCSPA, ORC 1345.02(A) prohibits "unfair or deceptive act[s] or practice[s] in connection with a consumer transaction."

518. Section 2 of the OCSPA, ORC 1345.02(B) defines certain unfair, unconscionable, or deceptive methods, acts, or practices, including but not limited to representing "[t]hat a consumer transaction involves or does not involve a warranty, a disclaimer of warranties or other rights, remedies, or obligations if the representation is false." ORC 1345.02(B)(10).

519. Defendant represented to consumers that it protects the personal information of Ohio residents, either implicitly by collecting such personal information or explicitly.

520. Contrary to these representations, intruders were able to gain access to personal information on Defendant's network and the Defendant suffered a data breach. Such representations were likely to mislead consumers acting reasonably under the circumstances into believing that personal information was safeguarded from misuse by third parties and were material to their decisions about whether to entrust the Defendant with personal information, including credit card information.

521. Defendant represented on its website that it accepted payments by credit card thus implicitly represented that it was compliant with the Payment Card Industry Data Security Standard ("PCI DSS"), which is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment to safeguard such information throughout the transaction process.

522. Contrary to these representations the Defendant was not in compliance with the Payment Card Industry Data Security Standard.

523. Defendant, in the course of conducting its business, failed to implement and maintain reasonable security procedures and practices appropriate to protect the personal information of Ohio residents that Defendant owned, licensed, or maintained, and thus did not protect that personal information from unauthorized access, use, destruction, modification, or disclosure.

524. The Defendant's misleading statements to consumers regarding its data protection practices have had the capacity, tendency, or effect of deceiving or misleading consumers and constitute unfair or deceptive trade practices as defined in ORC 1345.02(B)(10).

525. Defendant engaged in the acts and practices alleged herein when it knew or should have known that its conduct was unfair or deceptive, in violation of ORC 1345.02(A).

## DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Complaint so triable.

## REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually on behalf of himself and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Temu, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering Temu to pay actual damages to Plaintiffs and the other members of the Class;

C. Ordering Temu to pay for not less than three years of credit card monitoring services for Plaintiffs and the other members of the Class;

D. Ordering Temu to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

E. Ordering Temu to pay statutory damages, as provided by the New York Deceptive Acts and Practices Law and other applicable State Consumer Fraud Acts, to Plaintiffs and the other members of the Class;

F. Entry of an order for injunctive and declaratory relief as described herein, including but not limited to: i. enjoining Defendant, their affiliates, associates, officers, employees and

agents from transmitting Temu user data and content to China, to other locations or facilities where such Temu user data and content is accessible from within China, and/or to anyone outside the defendant companies;

G. Enjoining Defendant, their affiliates, associates, officers, employees and agents from taking Temu users' biometric identifiers and information without advanced notice to, and the prior written consent of, such Temu users or their legally authorized representatives (and, for the Illinois Subclass, without being in compliance with BIPA);

H. Enjoining Defendant, their affiliates, associates, officers, employees and agents from taking physical/digital location tracking data, device ID data, personally identifiable data and any other Temu user data and content except that for which appropriate notice and consent is provided and which Defendant can show to be reasonably necessary for the lawful operation of the Temu app within the United States;

I. Mandating that Defendant, their affiliates, associates, officers, employees and agents implement protocols to ensure that no Temu user data and content is transmitted to, or otherwise accessible from within, China;

J. Mandating that Defendant, their affiliates, associates, officers, employees and agents hire third-party monitors for a period of at least three years to ensure that all of the above steps have been taken; and

K. Mandating that Defendant, their affiliates, associates, officers, employees and agents provide written verifications on a quarterly basis to the court and counsel for the Plaintiffs in the form of a declaration under oath that the above steps have been satisfied.

L. Plaintiffs and subclass seek actual damages under RCW 19.06.090 and civil penalties under 19.86.140

M. Plaintiffs and subclass seek relief under ORC 1346.09

N. Ordering Temu to disseminate individualized notice of the Breach to all Class members;

O. Ordering Temu to pay attorneys' fees and litigation costs to Plaintiffs and the other members of the Class;

P. Ordering Temu to pay both pre- and post-judgment interest on any amounts awarded; and

Q. Ordering such other and further relief as may be just and proper.

Dated: Flushing, NY
February 19, 2024

Respectfully submitted,
*Attorneys for Plaintiffs*
TROY LAW, PLLC

*/s/ John Troy*

John Troy, Esq.
Tiffany Troy, Esq.
Aaron B. Schweitzer, Esq.
41-25 Kissena Boulevard
Suite 110
Flushing, NY 11355
(718) 762-1324
troylaw@troypllc.com

CHUNG LAW FIRM, P.C.
James Chung, Esq.
43-22 216th Street
Bayside, NY 11361
(718) 461-8808
jchung_77@msn.com

SHEEHAN & ASSCOIATES, P.C.
Spencer Sheehan, Esq.
60 Cutter Mill Road
Suite 412
Great Neck, NY 11021
(516) 268-7080
spencer@spencersheehan.com