# EXHIBIT A

PACIFIC TRIAL ATTORNEYS
A Professional Corporation
Scott J. Ferrell, Bar No. 202091
sferrell@pacifictrialattorneys.com
Victoria C. Knowles, Bar No. 277231
vknowles@pacifictrialattorneys.com
4100 Newport Place Drive, Ste. 800
Newport Beach, CA 92660
Tel: (949) 706-6464

Attorneys for Plaintiffs



**SUPERIOR COURT OF THE STATE OF CALIFORNIA**

**FOR THE COUNTY OF LOS ANGELES**

DALLAS POTTISH, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

WHALECO INC., a Delaware corporation, d/b/a TEMU.COM,

Defendant.

Case No. 26STCV13488

**CLASS ACTION COMPLAINT FOR UNLAWFUL SPAMMING AND INVASION OF PRIVACY**

## I. NATURE OF ACTION

1. Defendant WHALECO INC d/b/a TEMU.COM ("TEMU.COM") blankets California consumers with illegal spam. It deploys every deceptive tactic in the proverbial playbook — materially false subject lines, deceptive headers, and spoofed domains — to trick unwary Californians into opening messages they would otherwise ignore. In short, Defendant is the definition of a company that profits from modern spam abuse.

2. The harm does not stop at the inbox. After being deceived into engaging with the spam, Plaintiff was funneled to the website **TEMU.COM** where Defendant installed a web of illegal tracking pixels on Plaintiff's device. Those tracking technologies enable Defendant and its partners to follow Plaintiff's behavior across the internet, converting a single deceptive email into ongoing digital surveillance. TEMU.COM does this to everyone who clicks on its spam.

3. Both the spam and the surveillance are illegal under California law.[1]

## II. PARTIES, JURISDICTION AND VENUE

4. Plaintiff is and was at all times mentioned herein a citizen of the State of California who received a misleading spam e-mail from Defendant and visited Defendant's website after engaging with the deceptive spam.

5. TEMU.COM is a company that operates an online marketplace. TEMU.COM has purposefully availed itself of the benefits of conducting business in California by promoting its services to California residents. TEMU.COM knowingly accepts and profits from the resulting California-based traffic and transactions. The claims asserted herein arise directly out of and relate to this California-directed conduct, rendering the exercise of personal jurisdiction over TEMU.COM in this forum both proper and consistent with traditional notions of fair play and substantial justice. Indeed, it is believed that TEMU.COM has over 10,000 customers in California.

[1] *See Hypertouch, Inc. v. ValueClick, Inc.*, 192 Cal. App. 4th 805, 829-30 (Cal. Ct. App. 2d Dist. 2011) (Section 17529.5 "impos[es] strict liability on advertisers who benefit from (and are the ultimate cause of) deceptive e-mails"); *Id*. at 822 (Section 17529.5 "does not require the plaintiff to prove that it relied on the deceptive commercial e-mail message or that it incurred damages as a result of the deceptive message"); Id at 821 ("Section 17529.5 … does not include any 'scienter' or intent requirement"); *Id*. at 820 ("[S]ection 17529.5 does not require the plaintiff to show that the defendant actually made a false or deceptive statement…. [B]y its plain terms, the statute is not limited to entities that actually send or initiate a deceptive commercial e-mail, but applies more broadly to any entity that advertises in those e-mails."; and *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891 (N.D. Cal. 2023), aff'd, 2024 WL 123456 (9th Cir. 2024) (holding that the California Invasion of Privacy Act applies to internet conduct).

6. TEMU.COM is also subject to jurisdiction in California based upon its tracking of California consumers. Specifically, TEMU.COM knowingly installed cookies and collected data from Plaintiff and class members that it could geolocate in California, and then monetized that data, which constituted purposeful direction towards California. *See Briskin v. Shopify, Inc.*, No. 22-15815 (9th Cir. Apr. 21, 2025) (en banc) (holding that a defendant purposefully directs conduct toward a forum where it knowingly collects, processes, and monetizes data from users it understands to be located in that forum, even absent a physical presence, and that such targeted data exploitation — through tools like cookies and tracking technologies — constitutes express aiming sufficient to support specific personal jurisdiction when the claims arise from that conduct).

7. As a court of general jurisdiction, this Court has subject matter jurisdiction over all issues presented.

8. Venue is proper in this County because Defendant is not a citizen of California and because many class members were injured in this County.

## III. FACTUAL ALLEGATIONS

9. Plaintiff is a California citizen and is the owner of the e-mail address dallaspottish@gmail.com. TEMU.COM spams plaintiff and other class members relentlessly. As just one example, Plaintiff recently received a spam e-mail from Defendant with a materially deceptive subject line, forged header, and spoofed domain. The spam is attached hereto as **Exhibit "A".**

10. Defendant spammed Plaintiff from a nonsensical e-mail address. Confused, and believing that the e-mail might be from a legitimate source rather than an anonymous mass-marketing campaign, Plaintiff opened the email. In an effort to determine the e-mail's origin and legitimacy, Plaintiff was induced to click on a link in the e-mail which led to Defendant's website. But for the deceptive falsified and misleading header information and spoofed domain, Plaintiff would not have opened the message or visited Defendant's website. In this way, the spam directly caused Plaintiff's interaction with Defendant's site, which was the intended result of the deceptive campaign.

11. The email's metadata and embedded code reflect multiple indicia of spam evasion and deceptive marketing practices. The message was transmitted through a third-party bulk mailing service and routed with a sending IP that failed authentication checks, including DKIM failure and DMARC

rejection, indicating spoofing. The email further employs layered tracking and obfuscation techniques, masking the true destination of hyperlinks and enabling user tracking. The body of the spam contains multiple invisible tracking pixels (1x1 images) designed to monitor recipient engagement without consent. Additionally, the sender uses a mismatched "From" and "Reply-To" configuration and routes messages through intermediary domains to obscure the true sender identity. Collectively, these technical characteristics demonstrate deliberate efforts to evade spam detection, conceal the sender's identity, and surreptitiously track recipients.

12. The preceding is just a single example of the spam that Defendant sends to class members. Based on publicly available sources, it is believed that TEMU.COM is responsible for over 10,000 spam e-mails to Californians each year.

13. The spam identified above is an "Unsolicited Commercial e-mail advertisement" because plaintiff had no pre-existing relationship with Defendant and because the e-mail was initiated for the purpose of advertising or promoting the lease, sale, rental, gift offer, or other disposition of any property, goods, services, or extension of credit. *See* Bus. & Prof. Code § 17529.1(c). Likewise, Plaintiff has never given "direct consent" to receive commercial e-mail advertisements from Defendant or its marketing agents.

14. The above spam violates Bus. & Prof. Code § 17529.5(a)(1) because the domain used in the "From" field — **privaterelay.appleid.com** — is a classic example of a falsified domain under California Business & Professions Code § 17529.5(a)(1) because it bears no logical, corporate, or publicly traceable relationship to Defendant. This tricked Plaintiff into opening and engaging with the e-mail by clicking on a link that took plaintiff to Defendant's website. The use of privaterelay.appleid.com as the sending domain i misrepresents the identity of the sender by substituting an Apple-controlled relay domain in place of the actual advertiser's domain, temu.com. While Apple's private relay system is designed to mask a user's personal email address for privacy purposes, its use here has the effect of obscuring the true origin of the commercial message and preventing the recipient from identifying or tracing the advertiser responsible for the email. A reasonable recipient would not associate privaterelay.appleid.com with Temu, thereby defeating the core purpose of the "From" field as a reliable indicator of source. By routing a commercial advertisement through an unrelated third-

party domain that conceals the advertiser's identity while still promoting Temu's products, the email creates a mismatch between the entity benefiting from the message and the domain appearing in the header, which is precisely the type of sender obfuscation and misrepresentation that § 17529.5 was enacted to prohibit.

15. The spam violates Bus. & Prof. Code § 17529.5(a)(2) because the header information is falsified and deceptive, including the use of a "from" name, return address, and domain that does not accurately identify the party who initiated the email. The deceptive header information tricked Plaintiff into engaging with the e-mail and visiting Defendant's website to investigate it. Likewise, nothing in the header permits a recipient — or a reasonable investigator using publicly available tools such as WHOIS — to determine who actually sent or authorized the email.

16. Most importantly, the spam violates Bus. and Prof. Code § 17529.5(a)(3) because the subject line **"$0.01 False Nails – Ends Soon"** is deceptive because it conveys both a false price representation and a false sense of urgency that do not reflect the actual offer. First, the claim that the product is available for "$0.01" is literally false where no such product is actually sold at that price, as plaintiff confirmed by scouring the website. This constitutes a classic false pricing scheme in which a nominal price is used as bait to induce the recipient to open the email and engage. Second, the phrase "Ends Soon" reinforces the deception by creating artificial urgency, implying a limited-time promotion that requires immediate action, when in reality no genuine time-limited sale exists. Third, if such a sale actually did exist, the subject line omits all material conditions necessary to obtain the advertised price — such as eligibility requirements, hidden costs, or the fact that the product is not actually available for one cent — thereby misleading reasonable consumers about both the nature and availability of the offer. Taken together, the fabricated price, false scarcity, and omission of key terms render the subject line materially misleading because it induces engagement under the false impression that the recipient can obtain false nails for $0.01 for a limited time, when no such bona fide offer exists.

17. Although a plaintiff need not plead or prove actual damages to bring a claim under the statute, Plaintiff has in fact suffered concrete, particularized harm as a result of Defendant's conduct. Plaintiff spent valuable time and attention investigating the misleading offer; searching the WHOIS database to learn who the e-mail came from; incurred opportunity costs and lost productivity; and

suffered depletion of device and network resources, including storage space, bandwidth usage on a metered data plan, and battery life.

18. The unauthorized domain name, misleading header and false subject line also invaded Plaintiff's privacy and disrupted the ordinary use and enjoyment of Plaintiff's email account, diminishing its value as a communication tool and necessitating additional filtering and security precautions. These injuries were directly caused by Defendant's unlawful email and are redressable by statutory and injunctive relief.

19. Defendant has not established and implemented, with due care, practices and procedures reasonably designed to effectively prevent unsolicited commercial e-mail advertisements. In fact, Defendant actively defies California law, as shown by the fact that Defendant continues to spam California residents despite the existence of this lawsuit.

20. Going from bad to worse, after luring Plaintiff to its website via misleading spam, Defendant illegally installed numerous tracking pixels ("Tracking Pixels") on Plaintiff's device that allow various *de facto* data brokers **(including Amplitude, Fastly, and Facebook Domain Insights)** to (1) intercept communications from Plaintiff and track Plaintiff across the internet and (2) use those communications to compile and sell deeply personal details about Plaintiff to the highest bidders. Defendant does this to ***everyone*** who it lures to its site.

21. In short, Defendant has installed the Tracking Pixels to track signals generated by internet users (thus operating as a "Trap and Trace" device) to compile the dossiers described above and sell the information to the highest bidders. By doing so, Defendant has violated California Penal Code § 638.51.

22. The Tracking Pixels use algorithms to analyze internet and device data and predict whether two or more devices are owned by the same person. Participating websites and apps then cater their advertisements based on a collective knowledge of the user's actions across all of their devices. The Tracking Pixels use data such as cookie IDs, operating system IDs, IP addresses, online registrations, and data from partnering publishers to develop a probability that different devices are shared by the same person.

23. The Tracking Pixels are used for advertising to consumers across devices, where a user is shown an ad on their mobile or tablet device based on websites they visited on a desktop. For example,

if an Android phone visits a website shortly after a desktop PC from the same home network, the Tracking Pixels will assess that there is a high probability that the two devices are operated by the same person and will show them similar ads on both devices. The Tracking Pixels also use cross-device analytics for things like location, timing, user behavior, and audience analysis.

24. The Tracking Pixels spyware activities described above are known as "fingerprinting." Put simply, the Tracking Pixels collect as much data as it can about otherwise anonymous visitors to Defendant's website and matches it with existing information that the Tracking Pixels have acquired and accumulated about hundreds of millions of Americans.

25. According to the esteemed Brennan Center for Justice, data brokers are "the main purveyors of surveillance capitalism" that "collect, assemble, and analyze personal information to create detailed profiles of individuals, which they then sell to "financial institutions and insurance firms…Advertising companies… predatory loan companies, stalkers, and scammers…foreign actors…and law enforcement and other government agencies including the FBI and the IRS."). *See* https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole (last accessed April 2026).

26. After receiving the deceptive spam, Plaintiff visited the Website to investigate and was unaware of the secret spyware being used to surveil visitors and monetize their personal information.

27. The Tracking Pixels (1) begin to collect information the moment a user lands on the TEMU.COM.com website before any pop-up or cookie banner advises users of the invasion or seeks their consent; and (2) request and transmit other identifying personal information to link a user's behavior on Defendant's website to the visitor's social media accounts and other devices.

## IV. CLASS ACTION ALLEGATIONS

28. Plaintiff brings this action on behalf of all persons similarly situated and seek certification of the following class:

**All California citizens who:**

**(1) received any commercial e-mail promoting any of Defendant's products or services at a California e-mail address where such email(s) contained: (1) a falsified, misrepresented, or forged domain name; (2) falsified,**

**misrepresented, or forged header information; or (3) false or misleading subject line or contents; or**

**(2) visited a website owned or operated by Defendant using a web browser or mobile device, and whose interactions, communications, or personally identifiable information were intercepted, collected, or transmitted to any data brokers through the use of tracking pixels, cookies, or similar technologies, without their knowledge or consent.**

29. The above-described class of persons shall hereafter be referred to as the "Class." Excluded from the Class are any and all past or present officers, directors, or employees of Defendant, any judge who presides over this action, and any partner or employee of Class Counsel. Plaintiff reserves the right to expand, limit, modify, or amend this class definition, including the addition of one or more subclasses, in connection with a motion for class certification, or at any other time, based upon, inter alia, changing circumstances and/or new facts obtained during discovery.

30. **Numerosity.** The Class is so numerous that joinder of all members in one action is impracticable. The exact number and identities of the members of the Class is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, but Plaintiff is informed and believes, and thereon, alleges that there are at least 100,000 members of the Class.

31. **Typicality.** Plaintiff's claims are typical of those of other members of the Class, all of whom have suffered similar harm due to Defendant's course of conduct described herein.

32. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class. Plaintiff has retained attorneys who are experienced in the handling of complex litigation and class actions, and intend to prosecute this action vigorously.

33. **Predominance of Common Questions of Law or Fact.** Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary among members of the Class, and which may be determined without reference to the individual circumstances of any member of the Class, include, but are not limited to, the following:

a. Whether Defendant sent unsolicited commercial e-mail to Class members;

b. Whether Defendant secretly tracked visitors to its website by installing pixels from data brokers.

34. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable.

35. **Ascertainability**. Defendant keeps computerized records of its sales and customers through, among other things, databases storing customer orders, customer order histories, customer profiles, customer loyalty programs, and general marketing programs. Defendant has one or more databases through which a significant majority of members of the Class may be identified and ascertained, and they maintain contact information, including email addresses.

## V. CAUSES OF ACTION

### FIRST CAUSE OF ACTION

### Violation of Cal. Business & Professions Code § 17529.5

36. Plaintiff received the above unsolicited commercial e-mail at a California e-mail address within one year prior to filing the Complaint at a California e-mail address.

37. As shown above, the spam violated one or more provisions of Section 17529.5.

38. Defendant is strictly liable for violation of Section 17529.5 for sending spam and is liable in the amount of $1,000 per spam per class member.

39. Defendant has not established and implemented, with due care, practices and procedures reasonably designed to effectively prevent unsolicited commercial e-mail advertisements that are in violation of Section 17529.5 that would justify a reduction in liquidated damages.

40. Plaintiff and every Class member who received any violative e-mail are entitled to $1,000 in liquidated damages per e-mail from Defendant (Cal. Bus. & Prof. Code § 17529.5(b)(1)(B)(ii)), and to recover reasonable attorney's fees and costs (Cal. Bus. & Prof. Code § 17529.5(b)(1)(C)).

### SECOND CAUSE OF ACTION

### Violations of the California Trap and Trace Law

### Cal. Penal Code § 638.51

41. California's Trap and Trace Law is part of the California Invasion of Privacy Act ("CIPA") codified at Cal. Penal Code 630, et. seq.

42. CIPA was enacted to curb "the invasion of privacy resulting from the continual and increasing use of" certain technologies determined to pose "a serious threat to the free exercise of personal liberties." CIPA extends civil liability for various means of surveillance using technology, including the installation of a trap and trace device.

43. A "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

44. California Penal Code § 638.51(a) provides that "a person may not install or use…a trap and trace device without first obtaining a court order.…"

45. Defendant uses multiple trap and trace process on the Website by deploying the Tracking Pixels on its Website because they capture routing, addressing and/or other signaling information of website visitors including Plaintiff.

46. Defendant did not obtain consent from Plaintiff or class members before using trap and trace technology to identify users of its Website and has violated section 638.51 and did not obtain a court order to do so.

47. CIPA imposes civil liability and statutory penalties for violations of section 638.51. Cal. Penal Code § 637.2.

**THIRD CAUSE OF ACTION**

**California Intrusion Upon Seclusion**

48. Defendant intentionally intruded upon the private affairs, concerns, and seclusion of Plaintiff by improperly accessing Plaintiff's personal information and using it for improper purposes, including by partnering with multiple data brokers to sell Plaintiff's and class members' private information to the highest bidder and them with behavioral advertising.

49. Defendant's intrusions upon the private affairs, concerns, and seclusion of Plaintiff and class members has been substantial and would be highly offensive to a reasonable person and constitute

an egregious breach of social norms, as is evidenced by countless consumer surveys, studies, and op-eds decrying the online tracking of website visitors, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, scholarly literature on consumers' reasonable expectations, and the penalties imposed by the FTC and other regulatory bodies.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff seeks judgment against Defendant as follows:

a. For an order certifying that the action be maintained as a class action, that Plaintiff be designated as class representatives, and that undersigned counsel be designated as class counsel;

b. For all available declaratory, legal, and equitable relief including injunctive relief;

c. For statutory damages;

d. For punitive damages;

e. For attorneys' fees and costs as allowed by law; and

f. For any and all other relief at law or equity that may be appropriate.

Dated: April 27, 2026

PACIFIC TRIAL ATTORNEYS, APC

By: _____
Scott J. Ferrell
Attorneys for Plaintiff and the Proposed Class

# EXHIBIT A

From: Temu <email_at_news_temuemail_com_qvrggb5nsk_5ae2001d@privaterelay.appleid.com>
Date: Wed, Apr 22, 2026 at 2:24 PM
Subject: $0.01 False nails ends soon
To: <qvrggb5nsk@privaterelay.appleid.com>

Find us on

NOTE: This is an automatically generated email, please do not reply.
Office address: Suite 355, 31 St. James Avenue, Boston,
Massachusetts -02116, USA Please note, returns will not be accepted at this address.
If you want to return items, please request a return and use Temu's label.
Click to view more details.

Please contact customer service if you have any questions.

Privacy & Cookie Policy | Terms & Conditions | Unsubscribe