Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Deborah De Villa (SBN 312564)
ddevilla@ahdootwolfson.com
Alyssa D. Brown (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
Tel: 310-474-9111
Fax: 310-474-8585

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TEA DATING ADVICE, INC., X CORP., and 4CHAN COMMUNITY SUPPORT LLC,

Defendants.

Case No. 3:25-cv-06325

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Tea Dating Advice Inc., X Corp., and 4chan Community Support LLC (collectively, "Defendants"):

INTRODUCTION

1. This case arises from one of the most catastrophic and ironic data breaches in the digital age—a "safety" app designed to protect women exposed their most sensitive personal information to the darkest corners of the internet. Tea Dating Advice, Inc. ("Tea"), which marketed itself as a sanctuary where women could anonymously warn each other about dangerous men, instead became the very threat it promised to protect against.

2. On July 25, 2025, the unthinkable happened. Tea's entire database of user verification data—72,000 images including government-issued IDs—sat completely exposed on the internet, accessible to anyone with a web browser. *See* Zack Whittaker, *Women's Safety App Tea Breached, Exposing 72,000 User Images*, TechCrunch (July 26, 2025), https://techcrunch.com/2025/07/26/dating-safety-app-tea-breached-exposing-72000-user-images/; *see also* Joseph Cox, *Women Dating Safety App 'Tea' Breached, Users' IDs Posted to 4chan*, 404 Media (July 25, 2025), https://www.404media.co/women-dating-safety-app-tea-breached-users-ids-posted-to-4chan/. No password required. No authentication needed. Just click and download the most sensitive personal information of women who trusted Tea with their safety.

3. The breach was discovered not by Tea's security team, not by ethical hackers, but by anonymous users on 4chan—the notorious imageboard known for harassment campaigns against women. *See* Caitlin Dewey, *The Only Guide to 4chan You'll Ever Need*, Wash. Post (May 25, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/05/25/the-only-guide-to-4chan-youll-ever-need/. Within hours, these users had created automated scripts to systematically download every driver's license, every passport, every verification selfie. "DRIVERS LICENSES AND FACE PICS! GET THE FUCK IN HERE BEFORE THEY SHUT IT DOWN!" read the original post that set off a digital feeding frenzy. Cox, *supra*; *see also* Lorenzo Franceschi-Bicchierai, *Hackers Leak 13,000 User Photos*

and IDs from the Tea App, NBC News (July 26, 2025), https://www.nbcnews.com/tech/social-media/tea-app-hacked-13000-photos-leaked-4chan-call-action-rcna221139.

4. The data didn't stop at 4chan. Posts on Defendant X Corp.'s platform (formerly Twitter) amplified the breach, with users creating searchable databases linking women's real identities to their anonymous posts. "The drivers licenses leaked today from the tea app have been uploaded to a searchable map…. this may be the worst PII leak I've ever seen lol", one X post boasted. What was meant to be a shield for vulnerable women became a weapon in the hands of those who would do them harm.

5. For Plaintiff Jane Doe and tens of thousands of women like her, the nightmare was just beginning. Jane had joined Tea for one simple reason: she wanted to anonymously warn other women in her Northern California community about a man who sexually assaulted at least two other women. The app promised her that anonymity. It promised her safety. It promised to delete her verification data. Tea broke every one of those promises.

6. Instead of protecting women like Jane, Tea's shocking security failures handed their identities to the very predators they sought to avoid. The exposed data created a perfect kit for identity theft: high-resolution government IDs showing full names and addresses and selfies, many including EXIF location information too, among other sensitive and private information. For women who used Tea to report dangerous men, the breach didn't just compromise their financial security—it potentially exposed them to physical danger from the very people they were warning others about – now with maps of Tea users floating around the darker corners of the web. There is also public online humiliation of the sexist, sexual, and violent kind, and the potential for deepfakes. *See* Karen Hao, *Deepfake Porn Is Ruining Women's Lives. Now the Law May Finally Ban It*, MIT Tech. Rev. (Feb. 12, 2021), https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/.

7. How did this happen? Through a level of negligence so profound it defies belief. Tea stored its most sensitive user data in a Google Firebase storage bucket configured for completely public access. *See* Google Cloud, *Security Rules for Cloud Storage*, Firebase Documentation (last visited July 28, 2025), https://firebase.google.com/docs/storage/security. This wasn't a sophisticated hack. This was the digital equivalent of leaving the bank vault door wide open with a neon sign saying "Free Money Inside."

8. The catastrophic result is predictable: Firebase buckets that default to public access, exposing everything inside to the entire internet. What makes this breach particularly egregious is that Firebase security misconfigurations are so common, they've become a running joke in the cybersecurity community. *See* Dylan Curran, *Tea App That Claimed to Protect Women Exposes 72,000 IDs in Epic Security Fail*, Decrypt (July 26, 2025), https://decrypt.co/331961/tea-app-claimed-protect-women-exposes-72000-ids-epic-security-fail. Any competent developer knows to check these settings. Tea didn't bother.

9. When Tea finally acknowledged the breach—not through direct emails to affected users, but through an Instagram post—they had the audacity to call this a "legacy data storage system." Tea Dating Advice, Inc. (@theteapartygirls), Instagram (July 25, 2025), https://www.instagram.com/p/[specific-post-id]; *see also July 25th, 2025 Post by the Official Tea App Instagram Page*, Know Your Meme (July 26, 2025), https://knowyourmeme.com/photos/3108083-the-tea-app-data-leak. They claimed they kept this data "in compliance with law enforcement requirements." But evidence will show this was simply abandoned data, forgotten in an unsecured bucket, waiting to be discovered by anyone who looked.

10. This lawsuit seeks to hold all responsible parties accountable—not just Tea for its catastrophic security failures, but also X Corp. for allowing the widespread dissemination of stolen personal data on its platform, and 4chan Community Support LLC for enabling the coordinated theft and distribution of sensitive identity documents. In an age where data breaches have become commonplace, this case stands out for the particular cruelty of its impact: a safety app that made its users less safe, an anonymity platform that exposed identities, social media platforms that weaponized stolen data, and a tool meant to protect women that instead delivered their personal information to those who would do them harm.

11. Plaintiff brings this action individually and on behalf of all Tea users whose personal information was exposed in the breach, seeking damages, restitution, and injunctive relief to prevent such a betrayal from ever happening again.

PARTIES

Plaintiff

12. Plaintiff Jane Doe is a natural person and resident of a small community in Northern California. To protect her safety and privacy—ironically, the very things Defendant Tea promised but failed to provide—Plaintiff proceeds under a pseudonym. Given the nature of this breach and the sensitive information exposed, Plaintiff has a substantial privacy interest that outweighs the public's interest in knowing her identity.

13. Plaintiff began using the Tea app in or around February 2024. Plaintiff was required to provide, and did provide, her sensitive PII to Defendant Tea in order to use the Tea app. As a result of the Data Breach, Plaintiff's PII, including her driver's license information, was exposed to unauthorized third parties.

14. Plaintiff downloaded and joined Tea because she wanted to warn other women about a man who allegedly sexually assaulted two women in her small community in Northern California. Plaintiff specifically chose Tea because it promised anonymous reporting—she could fulfill her moral obligation to warn others without exposing herself to potential retaliation. In order to use Tea, Plaintiff was required to submit a photo of her driver's license and additional information through the Tea app, which she did, and that photograph and information now have been released through the Data Breach. Plaintiff is afraid the man in question will soon find out that Plaintiff posted about his alleged assault on the Tea app. Accordingly, Plaintiff is in fear for her safety as a result of this Data Breach.

15. As a direct result of Tea's failures and the subsequent distribution of her data on X Corp.'s platform and through 4chan, Plaintiff has suffered and continues to suffer significant harm. She has spent and will spend considerable time and money on protective measures, including identity theft protection. She lives in constant fear that her exposed driver's license will be used for identity theft, that her biometric data will be used to create deepfakes or bypass security systems, or worst of all, that the man she reported will find out she exposed him on the app and seek retaliation. With Tea, anonymity was her only protection. Defendants stole that from her.

Defendants

16. Defendant Tea Dating Advice, Inc. is a Delaware corporation doing business as "Tea" or "Tea App," with its principal place of business at 201 Spear St., Suite 1100, San Francisco, California 94105. Tea operates a mobile application and online platform marketed as a "dating advice" and safety tool exclusively for women.

17. Tea launched with a deceptively simple premise: create a space where women could share their dating experiences and warn each other about problematic men. The app rocketed to the #1 position on the App Store within days of launch, capitalizing on women's legitimate safety concerns in the modern dating landscape. *See* Matt Brian, *Dating App That Lets Women 'Rate' Men Hits Number 1 on the App Store, Immediately Suffers Data Breach*, Gizmodo (July 26, 2025), https://gizmodo.com/dating-app-that-lets-women-rate-men-hits-number-1-on-the-app-store-immediately-suffers-data-breach-2000634647.

18. Central to Tea's business model was its promise of creating a "safe space" for women. Marketing materials emphasized anonymity, privacy, security, and sisterhood. *See* https://www.teaforwomen.com (last visited July 28, 2025). Tea positioned itself as the antidote to traditional dating apps that had failed to protect women's safety. This positioning was not mere puffery—it was the core value proposition that convinced women to trust Tea with extraordinarily sensitive information.

19. Despite holding itself out as a guardian of women's safety, Tea is a venture-backed startup that prioritized rapid growth over basic security. Led by CEO Sean Cook, the company raised funding based on explosive user growth numbers while apparently devoting minimal resources to data security. Brian, *supra* (reporting "4 million users with another 900,000 on the waitlist"). When the breach was discovered, Cook went into hiding—refusing to respond to media inquiries or provide any public explanation for his company's catastrophic failures. Cox, *supra*.

20. Defendant X Corp. is a Nevada corporation with its principal place of business in San Francisco, California. X Corp. owns and operates the social media platform formerly known as Twitter, which has become a primary vehicle for the dissemination of Tea users' stolen personal information. Despite knowledge of the breach and the sensitive nature of the exposed data, X Corp. has failed to take

adequate measures to prevent the continued spread of stolen driver's licenses and identity documents on its platform.

21. Defendant 4chan Community Support LLC is a Delaware limited liability company headquartered in Los Angeles, California. 4chan operates the notorious imageboard website where the Tea breach was first discovered and exploited. 4chan users not only discovered the vulnerability but actively coordinated the mass downloading and distribution of women's personal identification documents, creating searchable databases and automated scripts to maximize the harm to Tea's users.

22. At all relevant times, Defendants owned, operated, and controlled their respective platforms. Each Defendant made decisions that directly contributed to the exposure and ongoing harm from this breach. The security failures of Tea, combined with the amplification and distribution capabilities of X Corp. and 4chan, created a perfect storm that transformed a data breach into a permanent privacy catastrophe.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which: (a) there are 100 or more members in the proposed class; (b) members of the proposed class have a different citizenship from Defendants; and (c) the claims of the proposed class members exceed the sum or value of $5,000,000, exclusive of interest and costs.

24. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because Plaintiff brings claims under the Driver's Privacy Protection Act, 18 U.S.C. § 2721 et seq., which is a federal statute providing a private right of action.

25. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367 because those claims are so related to the federal claims that they form part of the same case or controversy and derive from a common nucleus of operative facts.

26. This Court has personal jurisdiction over all Defendants because each Defendant conducts substantial business in this District, has sufficient minimum contacts with California, and otherwise purposefully avails itself of the markets in California through its business activities. Tea and X Corp.

maintain their principal places of business in this District. 4chan markets its services to and has thousands of users in California. All Defendants' conduct had direct and foreseeable effects in this District.

27. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Defendants conduct substantial business in this District, market their services to residents of this District, and the data breach affected numerous residents of this District. Additionally, Defendants' negligent data security practices and failure to prevent dissemination of stolen data had direct and foreseeable effects in this District.

28. Venue is also proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

A. Tea's Meteoric Rise: From Safety App to Privacy Nightmare

29. Tea burst onto the scene in 2023 like a feminist fever dream come true. Finally, women had a platform designed for women, where they could share the unvarnished truth about their dating experiences without fear of retaliation, harassment, or judgment. The concept was revolutionary in its simplicity: a members-only community where verified women could rate and review men they had dated, warning others about red flags, dangerous behavior, or simply disappointing dinner conversation.

30. The timing was perfect. In an era of #MeToo awareness and growing consciousness about dating violence, Tea offered what traditional dating apps had failed to provide: a backchannel for women's safety. While apps like Tinder and Bumble focused on making matches, Tea focused on keeping women alive and unharmed. It was whisper network technology—the digital evolution of women pulling each other aside at parties to warn, "Stay away from that guy."

31. Tea's marketing brilliantly tapped into this zeitgeist. "Date Smarter. Date Safer," proclaimed the ads. "The app where women have each other's backs." Social media influencers shared stories of how Tea helped them avoid dangerous situations. The message resonated powerfully: in a world where one in three women experience physical or sexual violence, Tea was a necessary tool for survival.

32. The app's exclusive nature—only verified women could join—added to its appeal. This wasn't another platform where men could infiltrate and harass. This was a protected space, a digital

sanctuary. Tea marketed this exclusivity as both a feature and a security measure. "Every member is verified," the company boasted. "Every woman is real. Every review is honest." *Id.*

33. The numbers tell the story of Tea's explosive growth. Within days of launch, Tea claimed the #1 spot on the Apple App Store. By July 2025, the company boasted 4 million users with another 900,000 on the waitlist. Brian, *supra*. The media crowned Tea the next unicorn startup, the app that would revolutionize dating by putting women's safety first.

34. But behind the feminist messaging and slick marketing lay a disturbing reality: Tea was just another venture-backed startup chasing growth at any cost. The company's actual commitment to women's safety extended exactly as far as its marketing budget. When it came to the unglamorous, expensive work of securing user data, Tea took a different approach: do the absolute minimum and hope nobody notices.

B. <u>The Identity Verification Trap: How Tea Collected a Goldmine of Sensitive Data</u>

35. To join Tea's exclusive community, women had to pass through a stringent identity verification process. This wasn't a simple email confirmation or phone number verification. Tea demanded government-issued photo identification—driver's licenses, passports, state IDs, along with other sensitive and private information.

36. The process was invasive by design. Tea's instructions were specific: the ID had to be clearly visible, with all information readable. No obscuring personal information. No privacy protection. Just hand over the keys to your identity and trust that Tea would keep them safe.

37. For women like Plaintiff Jane Doe, this requirement created an agonizing dilemma. The very reason she needed Tea—to anonymously report a dangerous man—made her reluctant to provide such sensitive information. But Tea's marketing was persuasive. They promised the data would be stored securely. They promised it would be deleted after verification. They promised that sacrificing privacy during onboarding would guarantee anonymity when it mattered.

38. Tea knew exactly what it was collecting. A driver's license contains a treasure trove of personal information: full legal name, date of birth, home address, physical description, signature, and a unique license number tied to government databases. Paired with other sensitive information, this created a perfect package for identity thieves: everything needed to open credit accounts, bypass security systems,

or create convincing fake identities. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (recognizing unique risks of biometric data).

39. With these images and other sensitive information, criminals could potentially:

a. Create deepfake videos for fraud or harassment

b. Bypass facial recognition security systems

c. Impersonate victims in video calls with banks or government agencies

d. Build comprehensive profiles for stalking or doxxing

e. Sell "verified" identities on dark web marketplaces

See Rana Ayyub, *I Was The Victim Of A Deepfake Porn Plot Intended To Silence Me*, Huffington Post (Nov. 21, 2018), https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316; *see also* Hao, *supra*.

40. Tea understood these risks. Any company collecting such sensitive data in 2023-2025 knew the stakes. Data breaches had become so common they barely made headlines unless they were spectacular in scope or incompetence. Yet Tea proceeded to collect this information from numerous women, storing it all in one convenient location, protected by exactly nothing.

C. Firebase Fiasco: How Tea Left the Vault Door Wide Open

41. The technical details of Tea's security failure would be comedy if the consequences weren't so tragic. Tea stored its entire collection of user verification data—72,000 images—in a Google Firebase cloud storage bucket. Cox, *supra*; Whittaker, *supra*. For those unfamiliar with cloud storage, imagine a digital filing cabinet that can be configured to be locked tight or left wide open for anyone to rifle through. Tea chose the latter.

42. Firebase, Google's cloud platform, is actually a robust and secure service—when configured properly. Storage buckets, in particular, require developers to configure access restrictions. Google Cloud, *Security Rules for Cloud Storage*, *supra*.

43. Tea never cared. It left its Firebase bucket configured for completely public access. No authentication required. No access logs to track who was downloading data. No encryption to protect the

files. Just a URL that anyone could access, like leaving diamonds in a cardboard box on the sidewalk with a sign saying "Please don't take."

44. Security professionals have a term for this kind of configuration: "misconfigured S3 bucket" (named after Amazon's storage service, though the principle applies to all cloud storage). It's such a common vulnerability that security researchers regularly scan the internet looking for exposed buckets. There are automated tools that can find them. There are countless articles warning about them. There are horror stories of companies destroyed by them. *See* Google Cloud, *Best Practices for Cloud Storage*, Google Cloud Documentation (last visited July 28, 2025), https://cloud.google.com/storage/docs/best-practices. Yet Tea fell into the same trap that has caught countless others who prioritized speed and profits over security.

45. On the evening of July 25, 2025, users on 4chan's technology board (/g/) launched what they called a "raid" on Tea. Cox, *supra.* 4chan is an anonymous imageboard that has become synonymous with coordinated harassment campaigns, particularly against women. Dewey, *supra*. Its users have weaponized doxxing—publishing private information to enable harassment—into an art form. And Tea had just handed them the perfect ammunition.

46. The original post that started it all was a call to arms: Anonymous users discovered Tea's exposed Firebase bucket and immediately recognized the goldmine they'd found. "DRIVERS LICENSES AND FACE PICS! GET THE FUCK IN HERE BEFORE THEY SHUT IT DOWN!" screamed the post that would soon destroy thousands of women's privacy and security. Cox, *supra*; Franceschi-Bicchierai, *supra*.

47. What followed was a feeding frenzy of the worst kind. Anonymous users didn't just browse the exposed data—they systematically downloaded everything. They created automated scripts to scrape every image. They built torrents to ensure the data would live forever on peer-to-peer networks. They uploaded copies to file-sharing sites. Within hours, 72,000 images containing the most sensitive personal information of Tea's users had been scattered across the internet like dandelion seeds in the wind—impossible to retrieve, impossible to delete.

48. The 4chan users understood exactly what they had found. These weren't just random photos—they were identity verification goldmines. One anonymous poster bragged about the "quality" of

the data: "It's not just driver's licenses. Every pic has the girl holding her ID next to her face. You could do anything with these." 4chan /g/ Archive, *supra*. Another celebrated finding users from their local area: "Found 3 girls from my town lmaooooo." *Id.*

49. But the violation went deeper than identity theft. 4chan users cross-referenced the exposed IDs with Tea's public reviews, connecting real names and addresses to the anonymous warnings women had posted. They created searchable databases linking women's identities to their Tea profiles. They extracted location data from EXIF metadata to create maps of where Tea users lived. *See* Amanda Silberling, *Tea App Suffers Breach, Exposing Thousands of User Images*, Engadget (July 26, 2025), https://www.engadget.com/cybersecurity/tea-app-suffers-breach-exposing-thousands-of-user-images-190731414.html. They transformed a safety app into a stalker's paradise.

50. The breach might have been contained to 4chan's dark corners, but Defendant X Corp.'s platform ensured maximum exposure and harm. Within hours of the initial 4chan discovery, X users began posting screenshots of the stolen data, links to download sites, and cruel commentary mocking the exposed women.

51. Posts on X didn't just share the data—they weaponized it. Users created threads identifying specific women, posting their driver's licenses alongside their Tea profiles. The platform's algorithm amplified these posts, spreading them to thousands of users who might never have visited 4chan.

52. Despite the obvious violation of its terms of service and potential criminal nature of sharing stolen government IDs, X Corp. failed to take swift action. Posts containing links to the stolen data remained active for hours or days. Even when individual posts were removed, new ones appeared faster X cared to take them down. X Corp.'s inadequate response ensured that the stolen data reached a far wider audience than 4chan alone could have achieved.

53. Most damning, X Corp. failed to implement any systematic approach to preventing the spread of Tea breach data. While the platform has sophisticated systems for detecting copyrighted content or terrorist propaganda, it failed and continues to fail to prevent the mass distribution of stolen driver's licenses and identity documents. This failure transformed X from a social media platform into an accessory to identity theft on a massive scale.

54. As July 25 turned to July 26, Tea's servers registered the massive spike in traffic to their Firebase bucket. Automated systems should have flagged the suspicious activity—gigabytes of data being downloaded by unauthorized users. But Tea's security monitoring was apparently as robust as their data protection: nonexistent.

55. It wasn't until 404 Media, a cybersecurity news outlet, independently verified the breach and contacted Tea for comment that the company even acknowledged something had gone wrong. Cox, *supra*. Let that sink in: Tea learned about the massive breach of its users' most sensitive data from a reporter, not from their own security systems.

56. Tea's initial response was a masterclass in corporate cowardice. CEO Sean Cook, who had been eager to talk to media when Tea was riding high at #1 on the App Store, suddenly became unreachable. He didn't respond to emails. He didn't answer LinkedIn messages. He didn't pick up the phone. As women's identities spread across the dark corners of the internet, the man responsible for protecting them was nowhere to be found. *Id.*

57. When Tea finally issued a statement on July 25, it came not through direct notification to affected users—as required by law—but through an Instagram post on @theteapartygirls. The statement was a marvel of corporate minimization and misdirection:

> We discovered unauthorized access to an archived data system. If you signed up for Tea after February 2024, all your data is secure. We have engaged third-party cybersecurity experts and are working around the clock to secure our systems. At this time, we have implemented additional security measures and have fixed the data issue.

Tea Dating Advice, Inc. (@theteapartygirls), Instagram, *supra*; *July 25th, 2025 Post*, Know Your Meme, *supra*.

58. Notice what's missing from this statement: any acknowledgment of what data was exposed, any explanation of how it happened, any apology to the affected users, any practical guidance for protecting themselves, or any recognition of the unique dangers facing women whose identities had been exposed after reporting dangerous men.

59. Tea's claim that the exposed data was in a "legacy data storage system" was particularly galling. This wasn't some forgotten server in a dusty closet—this was their active Firebase bucket

containing verification data from users who joined just months earlier. Tea later claimed they retained this data "in compliance with law enforcement requirements related to cyberbullying prevention," but this explanation raises more questions than it answers. What law requires retaining driver's licenses and selfies indefinitely? Why store them in an unsecured bucket? Why not inform users their data would be retained?

60. Meanwhile, affected users like Plaintiff Jane Doe were left to discover the breach through news reports, left to their own devices to figure out the true scale of the data breach, the potential danger to themselves, and the meanst to protect themselves.

61. The contrast between Tea's marketing promises and their breach response could not be starker. The app that promised to "have women's backs" had stabbed them in the back. The platform that offered "safety" had created danger. The company that valued "sisterhood" had abandoned its sisters in their moment of greatest need.

D. <u>The Unique and Devastating Harm: When Safety Apps Become Weapons</u>

62. Data breaches have become so common that we risk becoming numb to their impact. Another million credit cards stolen. Another database of passwords exposed. But the Tea breach stands apart for the particularly cruel nature of its harm. This wasn't just data—it was trust. This wasn't just privacy—it was safety. This wasn't just another breach—it was a betrayal that put vulnerable women directly in harm's way.

63. Consider the typical Tea user: a woman who had experienced something troubling, dangerous, or traumatic in the dating world. Someone who felt a moral obligation to warn others but needed anonymity to do so safely. Someone like Plaintiff Jane Doe, who knew that in her small town, publicly accusing a man of sexual assault would make her a target. These women came to Tea because traditional systems had failed them. The police couldn't or wouldn't help. Social media was too public. Word-of-mouth was too limited. Tea promised a solution: anonymous warnings backed by verified identities.

64. Now consider what the breach means for these women:

a. **Identity Theft on Steroids**: The combination of driver's licenses and other private, sensitive information provides everything needed for sophisticated identity fraud. Unlike credit card numbers that can be cancelled or passwords

that can be changed, the biometric data in those government ID's and selfies is forever. *See Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019) ("Biometrics are biologically unique to the individual; they cannot be changed if compromised"); *see also* Patel, 932 F.3d at 1273.

b. **The Deepfake Nightmare**: In 2025, artificial intelligence can create convincing fake videos from a single photo. Women whose data was exposed now face the terrifying possibility of seeing themselves in pornographic deepfakes or fraudulent videos.

c. **Real-World Stalking Risks**: For women who reported dangerous men, the breach created immediate physical safety concerns. Their full names and home addresses are now connected to their Tea posts. The men they warned about—men who had already shown themselves capable of violence—now have a roadmap to their front doors.

d. **Small Town Privacy Destruction**: For users like Plaintiff in smaller communities, anonymity wasn't just a preference—it was protection. In towns where "everyone knows everyone," the ability to warn others without being identified was crucial. The breach destroyed that protection forever.

65. The psychological harm is equally devastating. Women who trusted Tea with their most sensitive information now live in constant fear. Every unknown phone call could be a stalker who found their number. Every piece of mail could be evidence of identity theft. Every knock on the door could be retaliation for a warning they posted. The safety app has made them perpetually unsafe. *See In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 55 (D.C. Cir. 2019) (recognizing ongoing harm from data breach).

66. Making matters worse, the data can never be fully contained. While a breached credit card can be cancelled, the images Tea exposed will circulate forever. They're on 4chan archives. They're in torrent files. They're on hard drives around the world. They're in the hands of people who wish these women harm. Cox, *supra*; Silberling, *supra*. No security service can protect against a threat that's already everywhere.

E. The Technical Post-Mortem: A Masterclass in What Not to Do

67. As security researchers and journalists investigated the breach, a pattern of shocking negligence emerged. This wasn't a sophisticated attack by nation-state hackers. This wasn't a zero-day vulnerability that no one could have anticipated. This was basic Security 101 stuff that Tea simply ignored.

68. First, the Firebase misconfiguration. Google's documentation is crystal clear about storage bucket security. The Firebase console literally has a section called "Security Rules" with templates for common scenarios. Google Cloud, *Security Rules for Cloud Storage*, *supra*. Setting proper access controls takes minutes. Tea either never bothered to look or looked and decided user security wasn't worth those minutes.

69. Second, the complete absence of monitoring. Tea had no idea their data was being massively exfiltrated until reporters told them. No alerts for unusual access patterns. No warnings about large download volumes. No logging of who was accessing what. It's like having a bank vault with no cameras, no alarms, and no guards.

70. Third, the data retention disaster. Even if Tea had some legitimate reason to keep verification data (which they've never adequately explained), why keep it all in one place? Why not encrypt it? Why not segregate it from production systems? Why not implement access controls so only specific employees could view it for specific reasons? The answer appears to be that Tea simply uploaded everything to Firebase and forgot about it.

71. Fourth, the "vibe coding" problem. Multiple security experts who reviewed the breach concluded that Tea likely used AI-generated code for their Firebase implementation. The telltale signs were all there: functional code that worked but lacked basic security considerations, default configurations left unchanged, no evidence of security review or testing. It's what happens when startups prioritize speed over safety, when they trust ChatGPT more than security professionals.

72. Perhaps most damning is what Tea did have resources for. While they couldn't spare the time to secure user data, they had plenty of resources for marketing. While they couldn't afford proper security monitoring, they could afford Super Bowl ad campaigns. While they couldn't hire security professionals, they could hire growth hackers. The breach wasn't caused by lack of resources—it was caused by lack of caring.

F. The Aftermath: A Privacy Disaster That Keeps Getting Worse

73. In the days and weeks following the initial breach, the situation continued to deteriorate. The data didn't just exist on 4chan—it spread like wildfire across X and the internet's darkest corners. Discord servers organized the data by geographic location.

74. Attempts to contain the spread proved futile. While major platforms like Reddit and Twitter would sometimes remove direct links when reported, the data had already been downloaded thousands of times. For every link taken down, ten more appeared. For every torrent removed, mirrors emerged. The internet's decentralized nature, usually a strength, became a nightmare for the women whose data was exposed.

75. The role of X Corp. and 4chan in perpetuating the harm cannot be overstated. These platforms didn't just host the stolen data—they provided the infrastructure for its weaponization. On X, users created "Tea Breach" accounts dedicated to exposing specific women. On 4chan, anonymous users built searchable databases and automated tools for finding local victims. The platforms' failure to act swiftly and decisively transformed a data breach into an ongoing campaign of harassment and abuse.

76. For Plaintiff Jane Doe, the ongoing nightmare manifests in daily anxiety. She's had to purchase identity theft protection and live with the constant fear that the man she warned about on Tea will discover her identity. In her small town, she can't simply move away or disappear. She's trapped in a prison of Tea's making, where every day brings new fears about how her exposed data might be used against her.

77. The breach also had a chilling effect on women's safety more broadly. News of Tea's failure spread quickly through women's communities. The message was clear: even apps specifically designed to protect women couldn't be trusted. The digital whisper network that Tea promised to enable had been compromised at its foundation. How many women chose not to warn others about dangerous men because they'd seen what happened to Tea users? How many predators escaped accountability because their victims were too afraid to speak up, even anonymously? The harm ripples outward in ways we'll never fully measure.

CLASS ALLEGATIONS

78. Plaintiff brings this action individually and as a class action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) on behalf of herself and the following class (the "Class"):

> All persons residing in the United States whose Personally Idtenifiable Information ("PII") was exposed in the Tea data breach announced on or about July 25, 2025.

79. Plaintiff brings this action individually and as a class action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) on behalf of herself and the following Subclass (the "Subclass"):

> All persons residing in the United States whose driver's licenses were exposed in the Tea data breach announced on or about July 25, 2025.

80. Excluded from the Class are Defendants, including any entity in which any Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by any Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of any Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families. Plaintiff reserves the right to expand, limit, modify, or amend the proposed Class definition before the Court determines whether certification is appropriate.

81. The Class meets the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the following reasons.

82. Numerosity. Although the exact number of Class members is uncertain, and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable, believed to amount to many thousands of persons. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and the Court. Information concerning the exact size of the putative class is within the possession of Defendant Tea. The parties will be able to identify each member of the Class through discovery, including through Defendant Tea's document production and/or related discovery.

83. Commonality. There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether and to what extent Defendant Tea had a duty to protect Plaintiff's and Class Members' PII.

b. Whether Defendant Tea breached its duty to protect Plaintiff's and Class Members' PII.

c. Whether Defendant Tea's data security systems prior to the Data Breach met the requirements of relevant laws;

d. Whether Defendant Tea's data security systems prior to the Data Breach met industry standards;

e. Whether Defendant X and Defendant 4chan to owed duties to prevent the dissemination of stolen PII on their platforms;

f. Whether Defendant X and Defendant 4chan to breached those duties by failing to take adequate measures to prevent the spread of Plaintiff's and Class Members' PII;

g. Whether the actions and or/inaction of Defendants caused Plaintiff's and Class Members' PII to be disclosed or compromised;

h. Whether Defendants were negligent;

i. Whether Plaintiff and other Class Members are entitled to injunctive relief, including injunctions requiring Defendant X and Defendant 4chan to remove any PII from the Data Breach from their platforms; and

j. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendants' conduct.

84. Typicality. All of Plaintiff's claims are typical of the claims of the proposed Class she seeks to represent in that: Plaintiff's claims arise from the same practice or course of conduct that forms the basis of the Class claims; Plaintiff's claims are based upon the same legal and remedial theories as the proposed Class and involve similar factual circumstances; there is no antagonism between the interests of Plaintiff and absent Class Members; the injuries that Plaintiff suffered are similar to the injuries that Class Members have suffered.

85. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel experienced in complex class action litigation, including data breach and consumer protection cases. Plaintiff has no interests that are contrary to or in conflict with those of the Class.

86. Predominance. The proposed class action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Class predominate over any questions which may affect only individual Class members.

87. Superiority. The proposed class action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member. Absent a class action, the majority of Class Members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

88. Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendants. Varying adjudications could establish incompatible standards with respect to: whether Defendants' ongoing conduct violates the claims alleged herein; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other Class Members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

89. Injunctive Relief. This action also satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making injunctive and declaratory relief appropriate with respect to the Class as a whole. Class Members continue to face ongoing harm from the exposure of their PII and require injunctive relief to address Defendants' inadequate security practices, breach response, and failure to prevent ongoing dissemination of highly sensitive PII.

/ / /

/ / /

/ / /

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence
(On Behalf of Plaintiff and the Class Against All Defendants)

90. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

91. Defendant Tea required Plaintiff and the Class Members to submit highly sensitive, non-public PII to Defendant in order to use the Tea app.

92. Defendant Tea owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff's and Class Members' PII within its control from being compromised by or being accessed by unauthorized third parties. This duty arose from multiple sources, beginning with Defendant Tea's voluntary assumption of this duty by marketing itself as a "safety" app and promising to protect user data.

93. The duty was further established by the special relationship created when Defendant Tea required Plaintiff and Class Members to provide highly sensitive PII as a condition of using the Tea app. The foreseeable harm that would result from a breach of such sensitive information, particularly given Tea's user base of women reporting dangerous men, created an enhanced duty of care.

94. Defendant Tea alone was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and other Class members from the Data Breach.

95. In addition, Defendant Tea had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

96. Defendant Tea's duty to use reasonable care in protecting the PII arose not only as a result of the common law and the statutes and regulations described above, but also because it is bound by, and has committed to comply with, industry standards for the protection of confidential information.

97. Defendant Tea breached its common law, statutory, and other duties—and thus, was negligent—by failing to use reasonable measures to protect its customers' PII, and by failing to provide

timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class Members' PII;

b. failing to adequately monitor the security of its networks and systems; and

c. allowing unauthorized access to Plaintiff's and the Class Members' PII.

98. Defendant X and Defendant 4chan similarly owed duties to Plaintiff and Class Members once they became aware that stolen personal information was being disseminated on each of their platforms. These duties arose from the platforms' ability to control and remove content, combined with the foreseeability that failing to act would perpetuate and amplify the harm. Public policy against facilitating identity theft and harassment further established these duties, as did industry standards for content moderation and user protection.

99. Defendant Tea owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

100. It was foreseeable that Defendant Tea's failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

101. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

102. Defendants breached their duties of care through a cascade of failures. Defendant Tea knew or reasonably should have known of the inherent risks in collecting and storing the PII of Plaintiff and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the PII. Defendant Tea unlawfully breached its duty to use reasonable care to protect and secure the PII of Plaintiff and the Class by marketing the Tea app as "safe" and secure, and then failing to implement basic security measures to protect Plaintiff's and Class Members'PII.

103. Defendant X's breaches were equally serious. Defendant X failed to promptly remove posts containing stolen PII, allowed the creation of accounts dedicated to exposing Tea breach victims, and failed to implement systematic measures to prevent the spread of stolen PII. Most tellingly, Defendant X prioritized user engagement over user safety by allowing PII taken from the Data Breach go viral, treating stolen identity documents as just another form of trending content.

104. Defendant 4chan's breaches are also egregious. 4chan provided the platform and tools for coordinated theft of PII, failed to remove threads organizing the mass download of stolen PII, allowed users to create and share automated scripts for harvesting PII, and hosted searchable databases of victims' PII. Rather than acting as a neutral platform, 4chan became an active participant in the weaponization of stolen PII.

105. Defendants' breaches were substantial factors in causing Plaintiff's and Class Members' injuries. But for Tea's failure to implement basic security measures, the breach would not have occurred. But for X Corp.'s and 4chan's failure to prevent dissemination, the harm would have been contained. The causal chain is direct and unbroken.

106. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, among other things; (1) the exposure of their PII, including identification information such as home addresses, to online threat actors; (2) the loss of the ability to control how their PII is used; (3) compromise, publication and/or theft of Plaintiff's and Class Members' PII; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with their efforts expended

and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the Data Breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from PII misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) continued risks to their PII, which remains in Defendants' possession and may be subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (8) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the PII compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

107. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION

Negligence Per Se
(On Behalf of Plaintiff and the Class Against Defendant Tea)

108. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

109. Defendant Tea's duties arise from, *inter alia*, Section 5 of the FTCA, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Tea, of failing to employ reasonable measures to protect and secure PII.

110. Defendant Tea violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class Members' PII and not complying with applicable industry standards. Defendant Tea's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and other Class Members.

111. Defendant Tea's violation of Section 5 of the FTCA constitutes negligence *per se*.

112. Plaintiff and Class Members are within the class of persons that 5 of the FTCA was intended to protect.

113. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and other Class Members as a result of the Data Breach.

114. It was reasonably foreseeable to Defendant Tea that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

115. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

THIRD CAUSE OF ACTION

Invasion Of Privacy By Intrusion
(On Behalf of Plaintiff and the Class Against Defendant Tea)

116. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

117. The Restatement (Second) of Torts states:

> 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 (Second) of Torts § 652B (1977).

118. Plaintiff and the Class Members had a reasonable expectation of privacy in the PII Defendant Tea mishandled.

119. By intentionally failing to keep Plaintiff's and the Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant Tea intentionally invaded Plaintiff's and Class Members' privacy by intrusion.

120. Defendant Tea knew that ordinary persons in Plaintiff's or the Class Members' positions would consider this an invasion of privacy and Defendant's intentional actions highly offensive and objectionable.

121. Defendant Tea invaded Plaintiff's and the Class Members' right to privacy and intruded into Plaintiff's and the Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

122. Defendant Tea intentionally concealed from Plaintiff and the Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

123. In failing to protect Plaintiff's and the Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant tes acted with intentional malice and oppression and in conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private.

124. Plaintiff and the Class Members sustained damages (as outlined above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

FOURTH CAUSE OF ACTION

Breach Of Implied Contract
(On Behalf of Plaintiff and the Class Against Defendant Tea)

125. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

126. Plaintiff and members of the Class were required to provide, and did provide, their PII to Defendant Tea as a condition of using the Tea app.

127. Plaintiff and members of the Class had no alternative and did not have any bargaining power with regard to providing their PII. Defendant Tea required disclosure of their PII as a condition to access and use of the Tea app, which the Plaintiff and members of the Class did.

128. When Plaintiff and Class Members provided their PII to Defendant Tea in exchange for access and use of the Tea App, they entered into implied contracts with Defendant pursuant to which Defendant Tea agreed to safeguard and protect such PII and to timely and accurately notify them if their data had been breached and compromised.

129. Defendant Tea solicited prospective users to provide their PII as part of its regular business practices. These individuals accepted Defendant's offers and provided their PII to Defendant Tea. In entering into such implied contracts, Plaintiff and the Class reasonably assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant Tea would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

130. Plaintiff and the Class would not have provided and entrusted their PII to Defendant Tea in the absence of the implied contract between them and Defendant to keep the information secure.

131. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant Tea.

132. Defendant Tea breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Data Breach.

133. As a direct and proximate result of Defendant Tea's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

134. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

/ / /

/ / /

/ / /

FIFTH CAUSE OF ACTION

Violation Of The Driver's Privacy Protection Act, 18 U.S.C. §§ 2724, *et seq.*
(On Behalf of Plaintiff and the Subclass Against Defendant Tea)

135. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

136. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains . . . ." 18 U.S.C. § 2724.

137. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

138. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Driver's license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

139. Pursuant to the allegations herein, Defendant Tea knew or should have known that it obtained, disclosed or re-disclosed, and used PII from a motor vehicle record for a purpose not permitted under the DPPA.

140. By engaging in the conduct described above, Defendant Tea knowingly obtained personal information for a purpose not permitted under the DPPA.

141. By engaging in the conduct described above, Defendant Tea knowingly used personal information for a purpose not permitted under the DPPA.

142. By engaging in the conduct described above, Defendant Tea knowingly disclosed or re-disclosed personal information for a purpose not permitted under the DPPA.

143. As a result of Defendant Tea's acquisition, use, subsequent Data Breach, and violations of the DPPA, Plaintiff and putative Class Members are entitled to statutory damages to maximum allowable, actual damages, liquidated damages, and attorneys' fees and costs.

SIXTH CAUSE OF ACTION

Violations of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200 et seq.
(On Behalf of Plaintiff and the Class Against All Defendants)

144. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

145. Defendants are "persons" as that term is defined by, *inter alia*, Cal. Bus. & Prof. Code § 17201.

146. Defendants violated the California Unfair Competition Law ("UCL"), §§ 17200, *et seq*., by engaging in unlawful, unfair, and deceptive business acts and practices.

147. Defendants' unlawful, unfair, and deceptive acts and practices include: Defendants' failure to implement and maintain reasonable data security policies, practices, and measures to protect the PII of Plaintiff and Class Members from unauthorized access, disclosure, release, and theft, which was a direct and proximate cause of the Data Breach.

148. Defendant Tea failed to:

a. Secure access to its computer systems and database;

b. Comply with relevant industry standards for data and network security practices;

c. Adequately secure or segment its company network(s);

d. Implement adequate system and event monitoring over its computer systems;

e. Timely update and patch relevant programs related to its computer systems; and

f. Implement the systems, policies, and procedures necessary to prevent a foreseeable security intrusion such as the Data Breach.

149. Defendant Tea failed to identify and take adequate precautions against foreseeable security risks or to adequately improve its data security.

150. Defendant Tea's lackluster security provides little, if any utility, and is particularly unfair within the meaning of the UCL when weighed against the resultant harm to Plaintiff and Class Members.

151. Defendant Tea's lackluster security is also contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with it use appropriate security measures, as reflected in laws, including, *inter alia*, the FTCA, 15 U.S.C. § 45, California's Consumer

Records Act, Cal. Civ. Code §§ 1798.81.5, 1798.82, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*.

152. Defendant Tea's failure to implement and maintain reasonable data security policies, procedures, and measures, and Defendant X and Defendant 4chan failures to prevent the dissemination of stolen PII on their platforms; also lead to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition as contemplated under the UCL. Because Plaintiff and the Class Members did not and could not know of Defendants' inadequate security and compromise of their PII, they could not have reasonably avoided the harms caused by Defendants.

153. Defendants misrepresented that they would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, yet failed to do so. Defendants further omitted, suppressed, and/or concealed the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII.

154. Defendants misrepresented that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including all such duties as imposed by the FTCA, 15 U.S.C § 45; the DPPA, 18 U.S.C. §§ 2724, *et seq*.; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*., yet failed to do so. Defendants further omitted, suppressed, and/or concealed the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including the duties imposed by the aforementioned statutes.

155. Defendants engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

156. Defendants' misrepresentations and omissions to Plaintiff and the Class Members were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and ability to protect the privacy of their PII.

157. Defendants intended to mislead Plaintiff and members of the Class and induce them to rely on its misrepresentations and omissions.

158. If Defendant Tea had disclosed to Plaintiff and members of the Class that its computer and data systems were not secure and, thus, vulnerable to cyberattack, Defendant Tea would have been unable

to continue in business with such inadequate security policies, practices, and measures, and it would have been forced to adopt reasonable cybersecurity measures, in compliance with the law. However, Defendant Tea instead received, maintained, and compiled Plaintiff's and the Class Members' PII as a condition of using the Tea app without advising Plaintiff and Class Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant Tea's misrepresentations and omissions, the veracity of which they could not have discovered prior to the Data Breach.

159. Defendants acted intentionally, knowingly, and maliciously to violate the UCL in reckless disregard of Plaintiff's and Class Members' rights.

160. As a direct and proximate result of Defendants' violations of the UCL, Plaintiff and the Class sustained actual losses and damages as described herein.

161. Plaintiffs and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

162. Plaintiff brings this Cause of Action on behalf of all Class Members pursuant to UCL § 17203, which authorized extraterritorial application of the UCL.

SEVENTH CAUSE OF ACTION

Violation Of The California Consumer Records Act
Cal. Civ. Code §§ 1798.80, *et seq*.
(On Behalf of Plaintiff and the Class Against Defendant Tea)

163. Plaintiff incorporates the foregoing allegations as if fully set forth herein

164. The California Legislature enacted the California Consumer Records Act ("CRA"), Cal. Civ. Code §§ 1798.80, *et seq*., "to ensure that Personal Information about California residents is protected." Cal. Civ. Code § 1798.81.5(a)(1).

165. The CRA requires that "[a] business that owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

166. Defendant Tea maintains computerized data that includes PII, as defined by Cal. Civ. Code § 1798.80. This includes PII about Plaintiff and Class Members that was disclosed in the Data Breach. Cal. Civ. Code § 1798.81.5(d)(1)(A); Cal. Civ. Code § 1798.82.

167. Pursuant to the CRA, Defendant was required to "notify the owner or licensee of the information of the 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." Cal. Civ. Code § 1798.82(b). The security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

168. Defendant Tea reasonably believed that Plaintiff's and the California Sub-Class Members' PII was acquired by unauthorized persons during the Data Breach. As such, Defendant had an obligation under the CRA to disclose the Data Breach, immediately following its discovery, to Plaintiffs and California Sub-Class Members as the owners or licensees of the PII. Cal. Civ. Code § 1798.82.

169. By willfully, intentionally, and/or recklessly failing to disclose the Data Breach immediately following its discovery, Defendant Tea violated Cal. Civ. Code § 1798.82.

170. As a direct and proximate result of Defendan Teat's violations of the CRA, Plaintiffs and the California Sub-Class sustained actual losses and damages as described herein.

171. Plaintiff and the California Sub-Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

EIGHTH CAUSE OF ACTION

Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.150 *et seq.* ("CCPA")
(On Behalf Of Plaintiff the Class Against Defendant Tea)

172. Plaintiff incorporates the foregoing allegations as if fully set forth herein

173. This claim in pleaded on behalf of Plaintiff and the California Sub-Class.

174. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

175. Defendant Tea is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

176. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

177. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g).

178. Defendant Tea is a "business" as defined by Civ. Code § 1798.140(c) because it is a corporation that does business in the state of California and has annual revenues of in excess of $25,000,000.

179. Plaintiff's name in combination and other sensitive PII, compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA. *See* Civ. Code § 1798.150(a)(1).

180. Through the Data Breach, Plaintiff's PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

181. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

182. In accordance with Cal. Civ. Code § 1798.150(b)(1), prior to the filing of this Complaint, Plaintiff's counsel served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

183. If Defendant fails to respond to Plaintiff's notice letter or agree to rectify the violations detailed above and give notice to all affected consumers within 30 days of the date of written notice, Plaintiff also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant Tea's CCPA violations.

NINTH CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class Against Defendant X Corp.)

184. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

185. Defendant X Corp. entered into contracts with its users in connection with their use of the X's platform.

186. Under those contracts, Defendant X and its users agree to abide by the "X Rules"—which are in place to ensure all people can participate in the public conversation freely and safely.[1] In using the X platform:[2]

> **[Users] may not threaten to expose, incentivize others to expose, or publish or post other people's private information without their express authorization and permission, or share private media of individuals without their consent.**
>
> Sharing someone's private information online without their permission, sometimes called "doxxing," is a breach of their privacy and can pose serious safety and security risks for those affected.
>
> Additionally, posting images is an important part of our users' experience on X. However, where individuals have a reasonable expectation of privacy in an individual piece of media, we believe they should be able to determine whether or not it is shared. When we are notified by individuals depicted, or their authorized representative, that they did not consent to having media shared, we will remove the media. This policy is not applicable to public figures.[3]

187. Further, lists actions that may violate its policy, including:

> **What is in violation of this policy?**
> **Posting Private Information**
> You cannot share the following types of private information without the permission of the person it belongs to:
>
> - home address or physical location information, such as street addresses, GPS coordinates, or other identifying information related to locations that are considered private
> - identity documents, such as government-issued IDs or social security or other national identity numbers

[1] https://help.x.com/en/rules-and-policies/x-rules (last accessed July 28, 2025).

[2] https://help.x.com/en/rules-and-policies/personal-information (last accessed July 28, 2025).

[3] https://help.x.com/en/rules-and-policies/personal-information (last accessed July 28, 2025).

- contact information, such as non-public personal phone numbers, email addresses, or passwords
- financial account information, such as bank account or credit card details
- health-related private information, such as biometric data or medical records
- the identity of an anonymous user, such as their name or media depicting them

188. The contracts between Defendant X and its users was made expressly for the benefit of Plaintiff and Class Members. Plaintiffs and Class Members would rely on the contracts between Defendant X and its users to ensure the security of their sensitive and private PII was foreseeable to Defendant X.

189. "To help ensure people have an opportunity to see every side of an issue, there may be the rare occasion when we allow controversial content or behavior which may otherwise violate [X's] Rules to remain on our service because we believethere is a legitimate public interest in its availability. Each situation is evaluated on a case by case basis and ultimately decided upon by a cross-functional team."

190. Defendant X breached its contract with X users when it failed to protect Plaintiffs' and Class Members' PII from unauthorized dissemination in the X platform, among other things.

TENTH CAUSE OF ACTION

Declaratory and Injunctive Relief
(On Behalf of Plaintiff and the Class Against All Defendants)

191. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

192. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court may enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Moreover, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

193. An actual controversy exists between Plaintiff and Class members on one hand, and Defendants on the other, regarding Defendants' data security practices, content moderation obligations, and duties going forward.

194. The harm to Plaintiff and Class members is ongoing and irreparable. Their PII remains exposed on the internet and to cybercriminals. They face continuing risks of identity theft, fraud, stalking, and harassment. Without injunctive relief, Defendants are likely to continue their inadequate practices, putting current and future users at risk.

195. Plaintiff and Class members have no adequate remedy at law. Money damages cannot undo the exposure of their PII or eliminate the ongoing risks they face. Only prospective relief can prevent further harm and ensure Defendants implement adequate measures.

196. Plaintiff seeks a declaration that:

a. Defendant Tea's data security practices violated and continue to violate its legal obligations;

b. Defendants X Corp. and 4chan have obligations to prevent the dissemination of stolen personal information on their platforms;

c. All Defendants must implement comprehensive measures to protect users from data breaches and their consequences;

d. Defendant Tea must delete all unnecessary personal information in its possession;

e. All Defendants must provide transparent disclosures about their practices;

f. All Defendants must submit to regular audits by qualified third parties.

197. Plaintiff further seeks injunctive relief requiring Defendants to implement comprehensive remedial measures. As to Tea, Plaintiff seeks an order requiring immediate implementation of comprehensive information security measures, including encryption of all pii at rest and in transit, access controls limiting who can view sensitive data, regular security audits and penetration testing, employee training on data security, incident response procedures, and data minimization and retention policies. Tea must also delete all personal information that is no longer necessary for legitimate business purposes, provide clear and conspicuous notice to users about what data is collected, how it is used, how long it is retained, and how it is protected, implement a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information, and engage third-party security auditors to assess compliance and publish the results.

198. As to X Corp. and 4chan, Plaintiff seeks injunctive relief requiring these platforms to implement systems to detect and remove stolen PII including government IDs and other personally identifiable data from their platforms, develop and enforce policies prohibiting the dissemination of stolen personal information, and provide clear reporting mechanisms for victims of data breaches.

199. Plaintiff and Class Members continue to suffer injury as a result of Defendant's negligent exposure of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

200. Additionally, Plaintiff's and Class Members' PII, when contained in electronic form, is highly attractive to criminals who can nefariously use their PII for fraud, identity theft, and other crimes without their knowledge and consent.

201. Plaintiff seeks a judgment declaring:

a. That Defendant owes a legal duty to reasonably and adequately secure Plaintiff's and Class Members' PII.

b. That Defendant's past and present data security policies, practices, and measures do not comply with its contractual obligations and duties of care to reasonably and adequately secure Plaintiff's and Class Members' PII.

c. That Defendant continues to breach its contractual obligations and duties of care by failing to implement reasonable and adequate data security policies, practices, and measures to safeguard Plaintiff's and Class Members' PII.

202. Plaintiff further seeks an injunction from this Court compelling Defendant to implement cyber-security policies and procedures equal to or better than industry standards.

203. As alleged herein, the failures of the Defendant to implement adequate cyber-security measures and protocols has led to the compromise of the PII Plaintiff and members of the Class were required to provide as a condition of obtaining services from Defendant, resulting in irreparable harm.

204. Defendants remainsin possession of the PII of Plaintiff and the Class. It is imperative that the Court intervene to assure that the Defendant takes all reasonable steps to protect that PII lest there be another data breach.

205. The balance of equities tips decidedly in Plaintiff's favor. The burden on Defendants of implementing proper security and content moderation measures is minimal compared to the enormous ongoing harm to Class members from continued exposure of their personal information.

206. Injunctive relief would serve the public interest by protecting consumers' personal information, preventing the weaponization of data breaches, and enforcing minimum standards for companies that collect sensitive data and platforms that can amplify harm.

207. The hardship to Plaintiff and Class Members if such an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Absent an injunction, Plaintiff will likely be subjected to substantial identity theft and other damage, whereas the cost to Defendant of complying with an injunction by employing reasonable data security policies, practices, and measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment on behalf of herself and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing Plaintiff class representative and the undersigned counsel as Class Counsel to represent the putative Class;

b. Awarding Plaintiff and the Class appropriate relief, including actual damages, compensatory damages, and punitive damages, as allowed by law;

c. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

d. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

e. Awarding Plaintiff and the Class prejudgment and post-judgment interest;

f. Awarding Plaintiff and the Class their attorneys' fees and costs, as allowable by law; and

g. Awarding such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the Class, demands a trial by jury as to all issues triable of right.

DATED: July 28, 2025

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Deborah De Villa (SBN 312564)
ddevilla@ahdootwolfson.com
Alyssa D. Brown (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
Tel. (310) 474.9111
Fax: (310) 474.8585

Counsel for Plaintiff and the Proposed Class