UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JANE DOE, individually and on behalf of all others similarly situated, Plaintiff, v. TEA DATING ADVICE, INC., Defendant.	Civil Action No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jane Doe ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant Tea Dating Advice, Inc. ("TDA" or "Defendant"). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF THE CASE

1. Defendant Tea Dating Advice, Inc. developed the mobile application Tea Dating Advice ("Tea App" or the "App") with a clear goal in mind – "to give women the tools they need to date safely in a world that often overlooks their protection."[1]

2. The App is offered to women only and allows them to "share experiences and seek advice with a secure, anonymous platform."[2] Specifically, women users are able to take advantage of the App's safety tools, including background checks, catfish image searches, sex offender searches, phone number lookup, criminal record searches, and more.[3]

[1] https://www.teaforwomen.com/about
[2] https://www.teaforwomen.com/
[3] *Id.*

3. When women join the App, they are promised the App is safe. As Defendant's website touts, it is "the safest space to spill tea" given the App guarantees that users will be kept fully anonymous, does not permit screenshots, and verifies that all users are women.[4]

4. However, this is far from the truth. In the late afternoon of July 25, 2025, after it had already been widely reported online, Defendant posted an official statement to its website stating that it "identified unauthorized access to our systems[.]"[5] Defendant's statement went on to read:

> Preliminary findings indicate that the incident involved a legacy data storage system containing information from prior to February 2024. Approximately 72,000 images - including approximately 13,000 images of selfies or selfies featuring a photo identification submitted during account verification and 59,000 images publicly viewable in the app from posts, comments and direct messages - were accessed without authorization. We are currently working to determine the full nature and scope of information involved in the incident.

5. Just a few days later, on July 28, 2025, 404 Media, an online watchdog for these types of matters, published an article detailing a second breach of the App (referred to collectively with the July 25, 2025 breach as the "Breaches"). Specifically, an "independent security researcher now f[ound] it was possible for hackers to access messages between users discussing abortions, cheating partners, and phone numbers they sent to one another."[6] "The more than one million messages obtained by 404 Media are as recent as last week, discuss incredibly sensitive topics, and make it trivial to unmask some anonymous Tea users."[7]

6. Plaintiff brings this action against Defendant as a result of Defendant's failure to

---

[4] *Id.*
[5] https://www.teaforwomen.com/cyberincident
[6] https://www.404media.co/a-second-tea-breach-reveals-users-dms-about-abortions-and-cheating/
[7] *Id.*

safeguard and protect alleged "anonymous" information of Plaintiff and the other members of the Class, including photos of users' faces, information from government IDs that identifies users, users' posts, users' chats, and more (the "Sensitive Information").

7. Defendant's failure to safeguard and protect the Sensitive Information is in direct contrast to its own public representations, as well as representations made in its privacy policy, as more fully detailed below.

8. This lawsuit seeks to redress the public exposure of Plaintiff's and Class members' Sensitive Information.

PARTIES

9. Plaintiff Doe resides in New York, New York. In or around the beginning of 2024, Plaintiff signed up for the Tea App and in doing so, Plaintiff provided Defendant with her Sensitive Information, including a photo of her face.

10. Plaintiff is proceeding under a pseudonym in order protect her identity given the sensitive nature of this action, as outlined throughout.

11. Plaintiff signed up for and subsequently used the App because she wanted to gain access to Defendant'sdatabase and learn information that would keep her safe in her dating life. Plaintiff further used the App to warn other users about a dangerous experience she had with a man in New York City.

12. Plaintiff has posted her experiences with certain men on the App. Plaintiff also used the chat feature of the App to discuss a specific incident with a man with another user of the App. In doing so, Plaintiff shared personal information with the other user, which she believed would stay between herself and that user.

13. Plaintiff trusted Defendant with her Sensitive Information based on Defendant's

representations, including that the App was made to allow women to "share experiences and seek advice with a secure, anonymous platform." However, Plaintiff's Sensitive Information was neither secure nor anonymous, as it was leaked in the Breaches.

14. Defendant Tea Dating Advice, Inc. is a Delaware corporation with its principal place of business in San Francisco, California. As of July 2025, Defendant's App has over four million users in the United States.

JURISDICTION AND VENUE

15. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

16. This Court has personal jurisdiction over Defendant because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from this District, and because a substantial portion of the events giving rise to Plaintiff's claims occurred in this District, including Plaintiff's provision of her Sensitive Information to Defendant.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS

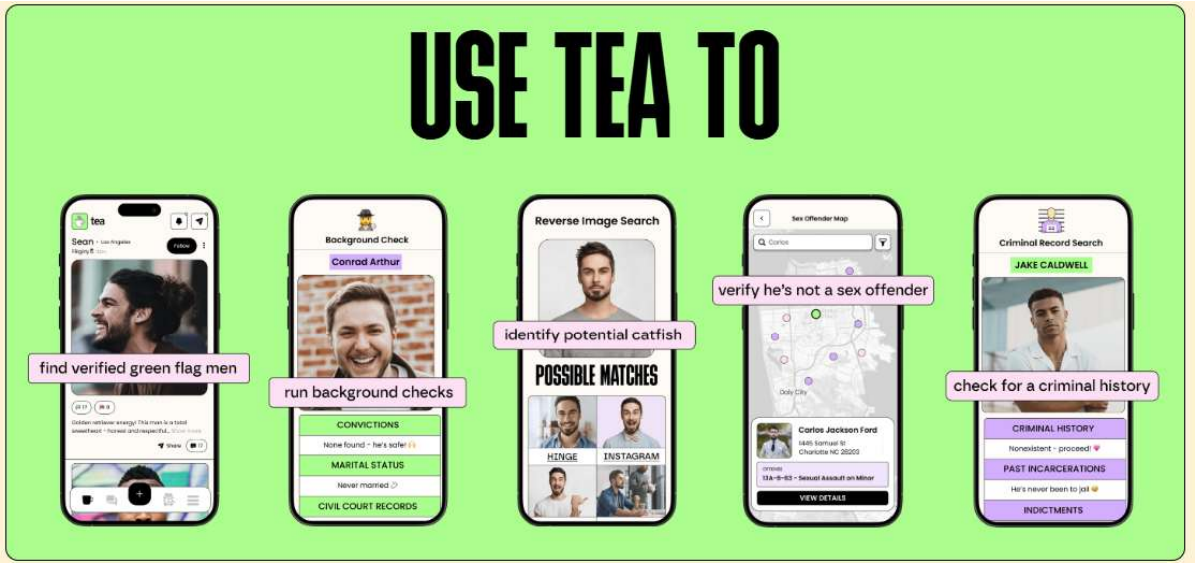
Defendant's Application

18. The Tea App aims to keep women safe and informed while navigating the dating scene. As the App's page on the application store explains: "Are we dating the same guy? Ask our anonymous community of women to make sure your date is safe, not a catfish, and not in a

relationship."[8]

19. To do so, "[u]sers can access a nationwide forum of posts and can set alerts for a man's name so you never miss any tea about your potential date, ex, or partner, and so you can make sure they are not a cheater. Users can anonymously ask for dating and relationship advice to find support and empowerment from our community of verified women."

20. Defendant's website and application store page advertises the following uses for the App:



21. Relevant here, Defendant's website touts that users can "[s]hare experiences and seek advice within a secure, anonymous platform." Users are further told that "Tea is built on trust; screenshots are blocked and all members are verified as women."

22. The following advertisement is also used by Defendant to promote user sign up and instill a sense of safety:

[8] https://apps.apple.com/us/app/tea-dating-advice/id6444453051?mt=8

23. The App also offers a chat function to users, allowing them to communicate privately and share personal information and experiences. Many users, including Plaintiff, rely on the chat function to reach out to other users to discuss an experience with an individual posted on the App, or to get more information on an individual posted on the App.

24. When signing up for the App, users are shown the following page explaining "How Tea Works":[9]

//

//

//

//

//

[9] Photos of the sign-up process were obtained by taking photos of an iPhone's screen due to the inability to screenshot on the App directly.

25. After proceeding past this screen, users are again shown the "Safety Tools" offered:

//

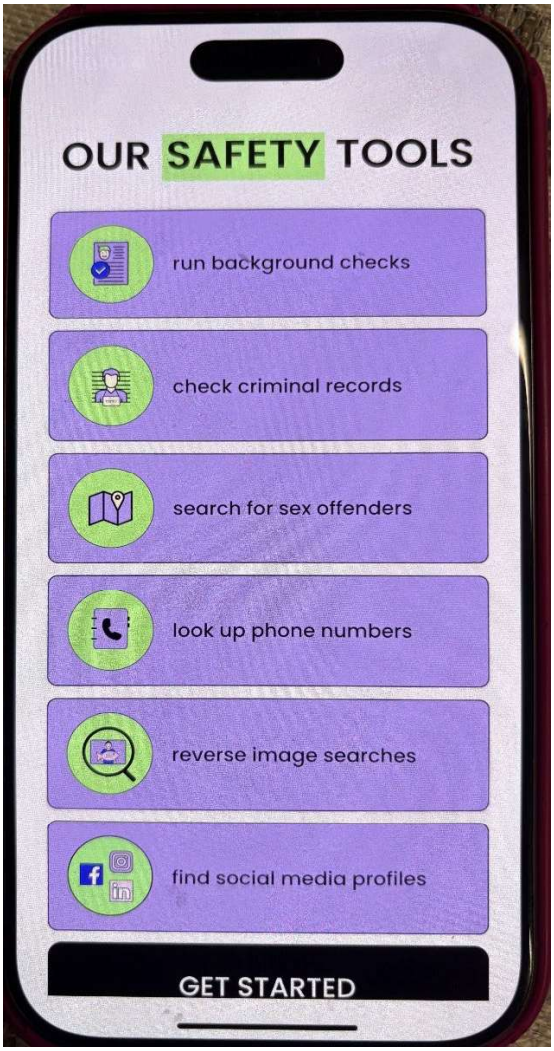
//

//

//

//

//



26. After clicking "GET STARTED," users are asked to provide their relationship status, the city they live in, and their date of birth. Users are also asked to create a username, which the App encourages to maintain anonymity.

27. Lastly, the App requires users to take a photo of their face, commonly referred to as a "selfie," for verification purposes. Notably, Defendant states that it will "delete it as soon as [the user] is approved."

//

//

//

28. Users are then submitted to a verification queue. Once the App verifies the selfie is indeed of a woman, the final step for users to gain access to the App is uploading their government ID.[10]

29. Indeed, as Defendant's privacy policy explains, "[w]hen you use or register with the Services, we may ask you to provide information by which you may be personally identified, such as your email address, date of birth, location, photograph, ID photograph, and any other identifier by which you may be contacted or identified online or offline[.]"[11]

[10] https://www.teaforwomen.com/terms ("When you first create a Tea account, we ask that you register by creating a username and including your location, birth date, photo and ID photo.").
[11] https://www.teaforwomen.com/privacy

30. Moreover, Defendant assures users that the uploaded selfie is "securely processed and stored only temporarily and will be deleted immediately following the completion of the verification process."[12]

31. The privacy policy provides further assurances to users:[13]

> We retain personal information we collect from You where we have an ongoing legitimate business need to do so (for example, to provide you with a service you have requested or to comply with applicable legal, tax, or accounting requirements). When we have no ongoing legitimate business need to process personal information, we will either delete or anonymize it or, if this is not possible (for example, because personal information has been stored in backup archives), then we will securely store personal information and isolate it from any further processing until deletion is possible.

32. The premise and purpose is clear – the App is meant to protect women by allowing them to anonymously rely on each other for intel, advice, warnings, and insight on the men they may encounter in the dating world. In doing so, Defendant promises their identity is safe.

33. As one review explains, the App "allows women to feel safe and not worry about the potential of meeting up with emotionally, psychologically, or physically abusive men that they've met online."[14] Another review provides, "[t]his is my safe space!!! It's a girls girls club and unlike the fb pages, everyone is nice … abusers, cheaters, liars, con men, std spreaders, married, all shared in a safe space to warn other women before their lives are ruined."

34. Defendant had obligations created by contract, industry standards, common law, and representations made to current, former, and prospective users to keep Plaintiff's and Class Members' Sensitive Information confidential and to protect it from unauthorized access and

---

[12] *Id.*
[13] *Id.*
[14] https://www.teaforwomen.com/reviews

disclosure. However, Defendant failed to uphold these obligations.

35. This was especially true in light of the polarizing views on the App. Aaron Minc, an attorney who specializes in online defamation and harassment, told *Reuters* that many men posted to the App have reached out in anger, stating that "[o]ver the last couple of weeks, we've gotten hundreds of calls on it. It's blown up. People are upset. They're getting named. They're getting shamed."[15]

Defendant Allowed Unauthorize Access to Plaintiff's and the Class' Sensitive Information

36. On the morning of July 25, 2025, posts on the website 4chan.org ("4chan") began to circulate regarding the ability to access Tea App users' Sensitive Information. 4chan, an anonymous, unregulated forum, is known for its users' extremist views and harmful content particularly towards women.[16]

37. In fact, in 2014, "a harassment campaign against women in gaming that resulted in bomb threats, death threats and women fleeing their homes" occurred on 4chan.[17]

38. Thus, when the post shown in the screenshot below was uploaded to 4chan, Tea users, including Plaintiff, were immediately afraid, rightfully so.

//

//

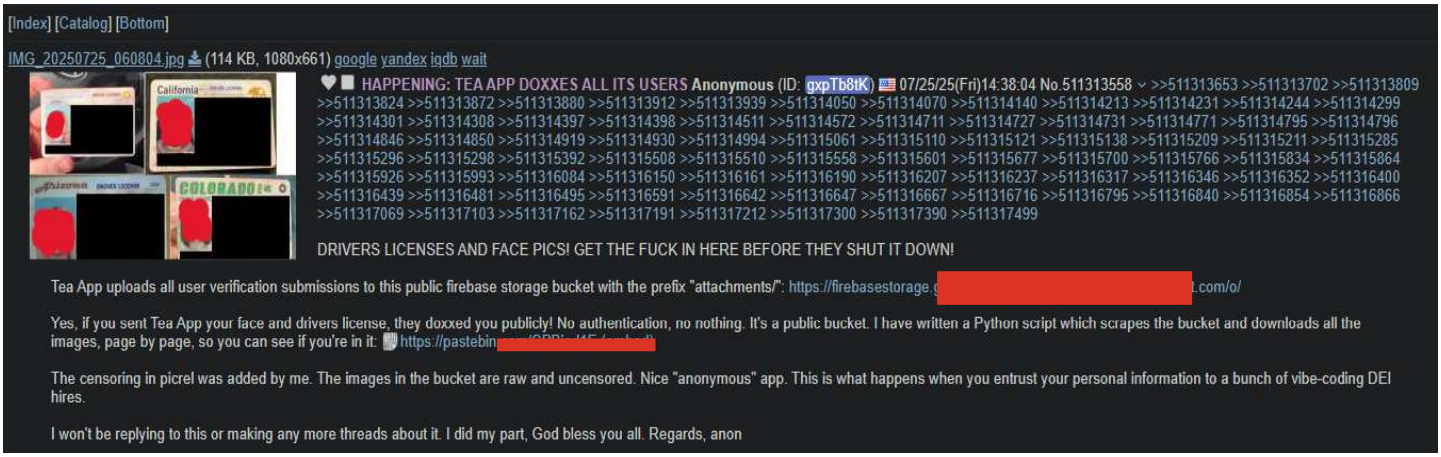
//

//

//

//

[15] https://www.livenowfox.com/news/tea-app-breach-fallout
[16] https://www.tandfonline.com/doi/full/10.1080/09546553.2024.2384044#abstract
[17] https://news.sky.com/story/is-this-the-end-of-notorious-4chan-internet-forum-13349823



39. As shown in the screenshot above,[18] thousands of users' Sensitive Information was spread on 4chan, including the selfies they took and the government IDs they uploaded for verification purposes.

40. As the post explains, "Tea App uploads user verification submissions to this public firebase storage bucket with the prefix 'attachments/." The 4chan user went on to explain, "[y]es, if you sent Tea App your face and drivers license, they doxed you publicly! No authentication, no nothing. It's a public bucket. I have written a Python script which scrapes the bucket and downloads all the images, page by page, so you can see if you're in it[.]"

41. The post also makes an alarming call to action: "DRIVERS LICENSES AND FACE PICS! GET THE FUCK IN HERE BEFORE THEY SHUT IT DOWN!"

42. 404 Media, an online watchdog that focuses on investigative reports regarding hacking, cybersecurity, and privacy generally, reported on the alleged breach shortly thereafter on July 25, 2024 at 11:18 am.

43. 404 Media verified the leak, stating that it "saw this list of files."[19] 404 Media

[18] The photos of licenses used in the 4chan post, as well as the URLs and hyperlinks directing users to the database, have been redacted for privacy reason.
[19] https://www.404media.co/women-dating-safety-app-tea-breached-users-ids-posted-to-4chan/

went on to explain "404 Media verified that Tea does contain the same storage bucket URL that 4chan claims was related to the exposure. 404 Media did this by downloading a copy of the Android version of the app and decompiling its code."[20]

44. 404 Media was not the only one accessing these files. Social media posts began to circulate rapidly, with maps purporting to link users' selfies and names to their addresses found on the licenses. As one X user wrote, "[t]he 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[.]"

45. Others were quick to acknowledge the unfortunate irony and dangers of the leak, with another X user posting "it says a lot like 'we made an app to help women share information about dangerous men' and then men's response to this was to get so upset they hacked it and publicly posted everyone's gov id[.]"

46. Social media was also replete with harmful dialogue directed at specific Tea App users. In one instance, an X account posted a screenshot of a Tea App user's license, calling her "a filthy, repugnant whore!"

47. "Posters across social-media platforms had a field day sharing Tea users' images, calling them 'whales' and 'ugly bitches,' saying that they deserved all of this."[21]

48. Even more jarring, a website was created for visitors to rank the selfies of Tea App users, as shown in the screenshot below:[22]

[20] *Id.*
[21] https://www.theatlantic.com/family/archive/2025/07/tea-app-dating-data-breach-misogyny/683712/
[22] The images of the Tea App users have been redacted for privacy purposes.

49. The backlash on Tea App users is unsurprising. In an article by The Atlantic titled "First Came Tea. Then Came the Male Rage," it explains "[w]hat Tea *has* accomplished, though, is showing what women are up against. The men so hell-bent on revenge against Tea's users are illustrating that hatred of women is alive and well. And the leaks demonstrated how insufficiently women are protected by the tech companies that shape their romantic lives."[23]

50. After the damage was done, Defendant posted an official statement to its website confirming that it "identified unauthorized access to our systems[.]" Defendant's statement went on to read:

[23] https://www.theatlantic.com/family/archive/2025/07/tea-app-dating-data-breach-misogyny/683712/

> Preliminary findings indicate that the incident involved a legacy data storage system containing information from prior to February 2024. Approximately 72,000 images - including approximately 13,000 images of selfies or selfies featuring a photo identification submitted during account verification and 59,000 images publicly viewable in the app from posts, comments and direct messages - were accessed without authorization. We are currently working to determine the full nature and scope of information involved in the incident.

51. However, the initial breach was only the beginning. Just a few days later, on July 28, 2025, 404 Media published a new article detailing a second breach of the App. Specifically, an "independent security researcher now f[ound] it was possible for hackers to access messages between users discussing abortions, cheating partners, and phone numbers they sent to one another."[24] The article went on to explain that "[t]he more than one million messages obtained by 404 Media are as recent as last week, discuss incredibly sensitive topics, and make it trivial to unmask some anonymous Tea users."[25]

52. 404 reported that its security researcher's findings revealed messages from early 2023 up until just this past week, with more than 1.1 million messages recorded and leaked.[26]

53. The article also stated the obvious – "It's hard to overstate how sensitive this data is and how it could put Tea's users at risk if it fell into the wrong hands."[27]

54. As a result of the second breach, the Tea App disabled users' ability to use the chat feature.

55. Media outlets from across the globe have since reported on this. As the New York Times explained, the App's "premise was immediately polarizing: Some praised it as a useful

---

[24] https://www.404media.co/a-second-tea-breach-reveals-users-dms-about-abortions-and-cheating/
[25] *Id.*
[26] *Id.*
[27] *Id.*

way to warn women about dangerous men, while others called it divisive and a violation of men's privacy."[28] This is why "[c]ritics[], including some users on 4chan, an anonymous message board known for spreading hateful content, called for the site to be hacked."[29]

56. Kevin Marriott, senior manager of cybersecurity firm Immersive, told the BBC "[t]he fact that criminals potentially have both images and the associated account's direct messages should raise the level of concern among users."[30] He went on to warn users that they should "remain vigilant as they wait to see what hackers plan to do with the stolen information."[31]

57. Ted Miracco, CEO at mobile security maker Approov, provided CBS News with his thoughts, stating that "[t]his is basic cybersecurity and something the company should be held accountable for … They rushed to market and promised consumers to create a safe site, and instead they exposed them."[32]

58. The App was not compromised by sophisticated parties that Defendant could not have foreseen targeting them. Instead, the App was accessed by amateurs that figured out the existence of the public database. Defendant failed to take reasonable measures, if any at all, to protect the women it promised to protect.

59. Firebase, Google's cloud platform Defendant used, is actually a robust and secure service—when configured properly. Storage buckets, in particular, require developers to configure access restrictions.

60. However, Defendant failed to uphold this requirement and instead left its Firebase

[28] https://www.nytimes.com/2025/07/26/us/tea-safety-dating-app-hack.html
[29] *Id.*
[30] https://www.bbc.com/news/articles/cd0dgkjgzvjo
[31] *Id.*
[32] https://www.cbsnews.com/news/tea-dating-advice-app-data-breach/

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. It cannot be determined how far information Defendant was entrusted to keep private has spread.

61. The backlash App users have received since their data was leaked has only just begun. Plaintiff and Class Members are in fear of what is to come. An App meant for women to feel safe and to protect them from men who may hurt them, harass them, stalk them, or worse, has now put them at risk of these exact harms. Their data, including their faces, identity, and addresses, has been put in the hands of men the App stood to protect them from, among others.

62. Even more alarming, Defendant was willfully unaware its users' Sensitive Information was accessible until it was made public.

63. Knowing the sensitive nature of the App, and the sensitive nature of their users' identities, Defendant should have taken reasonable measures to keep this information private. Defendant could have encrypted the Sensitive Information, could have stored it in internal databases, and could have aggregated it. But Defendant failed to take any measures at all, and in turn put Plaintiff and Class Members in danger.

64. Plaintiff's and Class Members' Sensitive Information was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

65. Defendant had a duty to adopt reasonable measures to protect the Sensitive Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its users' Sensitive Information safe and confidential.

66. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class

Members' Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure.

CLASS ALLEGATIONS

67. Plaintiff seeks to represent a class defined as:

> All women residing in the United States whose Sensitive Information was exposed to unauthorized actors by way of the data breach(es) on or about July 25, 2025 (the "Class").

68. Plaintiff additionally seeks to represent a subclass defined as "All members of the Class who are residents of New York." (Hereinafter, the "New York Subclass").

69. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

70. Excluded from the Class are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers and directors of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

71. This action seeks both injunctive relief and damages.

72. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

73. **Numerosity of the Class.** The Breaches affected tens of thousands of individuals. Therefore, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated from Defendant's records. If deemed necessary by the Court,

members of the Class may be notified of the pendency of this action.

74. **Existence and Predominance of Common Questions of Law and Fact.** There are question of law and fact common to the Class that predominate over any questions affecting only individual members, including:

(a) Whether Defendant's data security systems prior to the Breaches met the requirements of relevant laws;

(b) Whether Defendant's data security systems prior to the Breaches met industry standards;

(c) Whether Plaintiff's and other Class Members' Sensitive Information was compromised in the Breaches;

(d) Whether a reasonable consumer would believe the Tea App would protect their data and identity based on Defendant's representations; and

(e) Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

75. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

76. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel that is highly experienced in complex class action litigation, and Plaintiff intends to vigorously prosecute this action on behalf of the Class. Furthermore, Plaintiff has no interests that are antagonistic to those of the Class.

77. **Superiority.** A class action is superior to all other available means for the fair

and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense of individual litigation of their claims against Defendant. It would, thus, be virtually impossible for the Class on an individual basis, to obtain effective redress for the wrongs committed against them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances.

78. In the alternative, the Class may also be certified because:

(a) The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for the Defendant;

(b) The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

79. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

80. Defendant 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' Sensitive Information within its control from being compromised, including by being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate security measures over its networks so as to prevent unauthorized access thereof.

81. Defendant owed a duty of care to the Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that it adequately protected the Sensitive Information of the individuals who entrusted it to Defendant.

82. Only Defendant was in a position to ensure that its systems and the systems it utilized (i.e. Firebase) were sufficient to protect against harm to Plaintiff and members of the Class from the Data Breach.

83. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act, 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.

84. Defendant's duty to use reasonable care in protecting the Sensitive Information arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of Sensitive Information, as well as its own stated policies.

85. Defendant breached its common law, statutory, and other duties – and thus, was negligent – by failing to use reasonable measures to protect Plaintiff and Class Members' Sensitive Information, and by failing to abide by its own stated policies and representations. 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' Sensitive Information;

(b) Failing to adequately monitor the security of its networks and systems;

(c) Failing to abide by its own stated policies and representations with respect to Plaintiff's and the Class Members' Sensitive Information; and

(d) Allowing unauthorized access to Plaintiff's and the Class Members' Sensitive Information.

86. Defendant owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of any inadequate security practices. Defendant's App is meant to be an anonymous forum for women to freely share their experiences with men without the fear of repercussions and putting themselves in danger.

87. It was foreseeable that Defendant's failure to use reasonable measures to protect Sensitive Information 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.

88. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and

abuse, resulting in monetary loss, economic harm, emotional harm, and reputation damage; actual identity theft crimes, fraud, and abuse, resulting in monetary loss, economic harm, and physical harm; loss of confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; time spent monitoring their safety and identity information; lost work time; and other economic and non-economic harm.

89. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the Sensitive Information 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 Sensitive Information.

90. As a result of the foregoing, Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of Plaintiff and the Class which Plaintiff and members of the Class were required to provide to Defendant as a condition of using the App.

91. Plaintiff and members of the Class reasonably relied on Defendant to safeguard their information, and while Defendant was in a position to protect against harm from a data breach, Defendant negligently and carelessly squandered that opportunity. As a proximate result, Plaintiff and members of the Class suffered and continue to suffer the consequences of the Breaches.

92. Defendant's negligence was the proximate cause of harm to Plaintiff and members of the Class.

93. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information of its users, the Plaintiff's and Class Members' Sensitive Information would not have been exposed to unauthorized access and stolen, and they would not

have suffered any harm.

94. However, as a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class 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 loss of opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiff's and the Class Members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial accounts and/or likeness; (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 breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from data misuse; (6) unauthorized use of compromised Sensitive Information to open new financial accounts; (9) continued risks to their Sensitive Information, which remains in Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

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

COUNT II
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

96. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

97. Plaintiff and members of the Class provided Sensitive Information to Defendant in connection with their use of the App from Defendant and were required to provide their Sensitive Information as a condition of receiving services therefrom.

98. Defendant would not have enrolled Plaintiff in the App, nor enrolled any members of the Class, had Plaintiff and members of the Class not provided various forms of Sensitive Information to Defendant, including license information, photos of government IDs, photos of their faces, and other privileged and confidential items of information.

99. Plaintiff and members of the Class had no alternative and did not have any bargaining power with regards to providing their Sensitive Information. Defendant required disclosure of Sensitive Information as a condition to providing its services, which the Plaintiff and members of the Class did.

100. When Plaintiff and Class Members provided their Sensitive Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

101. Defendant solicited and invited prospective App users to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Sensitive Information to Defendant. In entering into such implied contracts, Plaintiff and the Class reasonably believed that Defendant's data security practices and

policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

102. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

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

104. Defendant breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Breaches.

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

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

COUNT III
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

107. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

108. Plaintiff and Class Members entered into written agreements with Defendant as part of, and as a precondition to, using the App. These agreements contained or incorporated the representations outlined *supra* ¶¶ 1-3, 15, 18, 24-28 that Defendant would protect and responsibly handle Plaintiff's and Class Members' Sensitive Information. The agreements

involved a mutual exchange of consideration whereby Defendant provided (or committed to considering to provide) use of the App for Plaintiff and Class Members in exchange for their Sensitive Information.

109. Defendant's failure to abide by its own stated policies and Defendant's failure to protect Class Members' Sensitive Information constitute a material breach of the terms of the agreement by Defendant, as reflected, *inter alia*, in its policies relating to Sensitive Information outlined *supra*.

110. As a direct and proximate result of Defendant's breach of contract with Plaintiff and Class Members, Plaintiff and Class Members have been irreparably harmed.

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

COUNT IV
Violation Of New York General Business Law § 349
(On Behalf of Plaintiff and the New York Subclass)

112. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

113. Defendant, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade, and commerce and the furnishing of services, in violation of N.Y. GBL § 349(a). This includes but is not limited to the following:

(a) Defendant failed to enact adequate privacy and security measures to protect the New York Subclass Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Breaches;

(b) Defendant failed to take proper action following known security risks which was

a direct and proximate cause of the Breaches;

(c) Defendant knowingly and deceptively misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

(d) Defendant knowingly and deceptively misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information; and

(e) Defendant failed to abide by its own stated policies pertaining to the privacy and security of Sensitive Information.

114. Moreover, Defendant made repeated representations to Plaintiff and New York Subclass Members in regard to the anonymous nature of the App and the promise to keep users safe, as outlined *supra* ¶¶ 1-3, 15, 18, 24-28.

115. Plaintiff and New York Subclass Members reasonably expected Defendant to abide by its own policies and representations.

116. As a direct and proximate result of Defendant's practices, Plaintiff and other New York Subclass Members suffered injury and/or damages, including, but not limited to, time and expenses related to monitoring their safety, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

117. The above unfair and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and other New York Subclass Members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

118. Defendant knew or should have known that its data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful.

119. Plaintiff, on behalf of herself and the putative New York Subclass, seeks relief under N.Y. GBL § 349(h) for the greater of actual damages (to be proven at trial) and statutory damages of $50 per violation, injunctive relief, and/or attorneys' fees and costs.

120. Plaintiff and New York Subclass Members seek to enjoin the unlawful deceptive acts and practices described above. Each New York Subclass Member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions, because, as detailed herein, Defendant will continue to fail to protect Sensitive Information entrusted to it.

121. Plaintiff and New York Subclass Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. GBL § 349.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For compensatory and punitive damages in amounts to be determined by the Court and/or jury;

(d) For prejudgment interest on all amounts awarded;

(e) For an order of restitution and all other forms of equitable monetary relief;

(f) For an order directing Defendant to cease the illegal actions detailed herein; and

(g) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

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 30, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Alec M. Leslie*
Alec M. Leslie

Alec M. Leslie
Spencer N. Migotsky
Caroline C. Donovan
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: aleslie@bursor.com
smigotsky@bursor.com
cdonovan@bursor.com

Counsel for Plaintiff