Israel David*
israel.david@davidllc.com
Blake Hunter Yagman*
blake.yagman@davidllc.com
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, New York 10004
Tel.: (212) 739-0622

*Pro Hac Vice Forthcoming

Attorneys for Plaintiff Gerber

Jeff Westerman, Esq. (CA Bar No. 94559)
jwesterman@jswlegal.com
WESTERMAN LAW CORP.
16133 Ventura Blvd., Suite 685
Encino, California 91436
Tel.: (310) 698-7450

Local Counsel for Plaintiff Gerber

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

STEPHEN GERBER, individually and on behalf of himself and all others similarly situated,

Plaintiff,

v.

TWITTER, INC.;

Defendant.

Case No. _____

CLASS ACTION

Claims for:
1. Negligence;
2. Breach of Contract; and,
3. Violations of California's Unfair Competition Law.

DEMAND FOR JURY TRIAL

Plaintiff Stephen Gerber ("Plaintiff"), individually and on behalf of himself and all other persons similarly situated, brings this Class Action Complaint (the "Action") against Defendant Twitter, Inc. ("Twitter" or the "Defendant"), and alleges upon personal knowledge as to his own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Twitter, in its most basic form, as a social media platform where users can post and digest short-form commentary, is a digital, modern-day version of the public square.

2. At the very core of Twitter's business model is its invitation to would-be Twitter users to join the Twitter platform and share their interests and views on myriad subjects, including politics, religion, sports, fashion, pets, food, sexuality, and everything in between. Twitter also offers the user the opportunity to share and engage anonymously. Users may use pseudonyms and other anonymous usernames so that they may express themselves and their opinions without fear of retaliation, embarrassment, or other repercussions from their employer(s), colleagues, acquaintances, neighbors or government.

3. Many tens of millions of Twitter users have accepted this invitation from Twitter. Although these Twitter users do not pay Twitter directly for the ability to use Twitter, these users collectively deliver enormous value (and profits) to Twitter. These users and the data generated by their use of the platform are Twitter's product. Advertisers generate billions in annual revenues for Twitter for the opportunity to reach these tens of millions of users. Additional billions in revenues are generated for Twitter by licensing certain data generated by its users. These revenue streams — generated directly by the users — are the basis for Twitters recent valuation of approximately $44 billion.

4. Twitter is obligated, and has promised to, protect certain private information entrusted to it by its users in order to access the platform and, in turn, provide Twitter with the source of its billions in revenues. However, from June 2021 through January 2022, a defect in Twitter's application programming interface ("API") allowed cybercriminals to exploit this defect

and "scrape" data from Twitter. The compromised information included users' Twitter usernames, email addresses and phone numbers (the "Personally Identifiable Information" or "PII") associated with specific Twitter accounts. The combined set of compromised information deanonymized the tens of millions of Twitter users — like Plaintiff and members of the putative Class – who wished to stay anonymous for the aforementioned reasons while using Twitter. It is particularly problematic to leak users' Twitter usernames ***in combination*** with email addresses and phone numbers as here, because that combination gives the person interpreting (or, more aptly, the cybercriminal abusing) the data the ability to link an otherwise anonymous or pseudo-anonymous username on Twitter with that particular user's generally not anonymized email address and/or phone number. For example, the Plaintiff in this matter used an anonymous Twitter username which was compromised in this incident in combination with his non-anonymous email address (which contains elements of his actual name). As a result, anyone who comes into possession of the combined compromised information can now relatively simply connect Plaintiff with his heretofore anonymous Twitter username.

5. This is not only a violation of Twitter's Privacy Policy (the "Privacy Policy"), and, therefore, Twitter's Terms of Service, but also violates a 2011 agreement between Twitter and the United States Federal Trade Commission which states:

> "[Twitter] shall not misrepresent in any manner, expressly or by implication, the extent to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information,[1] including but not limited to misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) to honor the privacy choices exercised by users."

6. The cache of information exposed by the API exploitation includes over 200,000,000 Twitter users' information including the aforementioned PII. Because of the anonymized, pseudo-anonymized and confidential nature of Twitter (which, as detailed above, is Twitter's core premise and value proposition to would-be users), these Twitter users were not only

[1] Defined as: "nonpublic, individually-identifiable information from or about an individual customer, including but not limited to an individual consumer's (a) email address… (c) mobile telephone number…"

misled by Twitter into thinking that they would remain publicly anonymous if they chose to do so, but that the PII underpinning their accounts would also remain safely guarded by Twitter.

7. To compound matters, Twitter seemingly buried its head in the sand regarding the magnitude of this API exploitation or, even worse, Twitter may have even taken actions intended to conceal the true magnitude of this API exploitation when they stated in August of 2022 regarding the API exploitation: "[w]hen we learned about this, we immediately investigated and fixed it. At that time, we had no evidence to suggest someone had taken advantage of the vulnerability." This is extremely problematic because it evidences that Twitter (which, to this day has inexplicably failed to notify or contact the victims of this particular API exploitation) refuses to acknowledge the seriousness of what has occurred. The PII belonging to victims of the API exploitation is now being disseminated and sold on the dark web by cybercriminals who mined the information, despite Twitter's representations and omissions to the contrary.

8. Twitter's conduct as alleged herein deceived Twitter users and exposed them to a multitude of harms related to Twitter's failure to protect their PII. As such, Plaintiff Gerber and the members of the putative Class bring this Action against Twitter for violations of state law to seek damages, inclusive of actual damages and restitution, injunctive and equitable relief, reasonable costs and attorneys' fees, and pre- and post- judgment interest.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this Action pursuant to the Class Action Fairness Act, 28 U.S.C. 1332(d), because this Action is a putative Class Action wherein the amount-in-controversy exceeds $5,000,000 exclusive of interest and costs and there are well more than 100 members of the putative class. In addition, at least one member of the class is a citizen of a different state from the Defendant – namely, Plaintiff Gerber is a New York resident and Defendant Twitter is a corporation which is headquartered in California and incorporated in and under the laws of the state of Delaware.

10. This Court has personal jurisdiction over the Defendant because Defendant maintains its principal place of business in this District, at 1355 Market Street, San Francisco,

California. Twitter has systematic and continuous contacts with the State of California, availing itself to the laws of California.

11. Venue is proper in this Court pursuant to 28 U.S.C. 1391 because the Defendant resides in this District and because a substantial part of the events giving rise to the claims herein occurred within this District. Additionally, Twitter's Terms of Service require that any and all disputes be heard in the state or federal courts located in San Francisco, California.

PARTIES

Plaintiff Stephen Gerber

12. Plaintiff Gerber is, and at all times relevant to this Action was, a resident of the state of New York.

13. Plaintiff Gerber was a Twitter user for several years prior to terminating his account in 2022. During the time period in which Plaintiff Gerber used Twitter, Plaintiff Gerber used a pseudonym as his Twitter username in order to protect his identity so that he could express himself and his thoughts on Twitter without fear of retribution, retaliation or embarrassment from employer(s) and his peers.

14. Plaintiff Gerber's PII was exposed by Twitter in the API scraping incident that took place from 2021-2022. Had Plaintiff Gerber been aware that Twitter would allow its cache of PII collected from Twitter's users to be exposed by cybercriminals, he either would not have provided his email address or other identifying information to Twitter or he otherwise would not have used Twitter at all.

Defendant Twitter, Inc.

15. Defendant Twitter Inc. is a corporation existing and organized under the laws of the state of Delaware. Twitter maintains its principal place of business at 1355 Market Street, San Francisco, California.

FACTUAL ALLEGATIONS

Defendant's Business and Privacy Policy

16. Twitter operates one of the largest social media platforms in the world.

17. The way that Twitter works is rather simple: users, after creating a Twitter account with a username and password, are able to broadcast short messages, called "Tweets" in order to share viewpoints, information, images, or videos with other Twitter users. Additionally, Twitter users are displayed a "mini-feed" of Tweets by other users that they either follow or that Twitter's algorithm finds to be relevant to them so that the users can view and interact with these Tweets either by "liking" them, reposting them (called a 'Retweet') or by commenting on them. Twitter users are also given access to a search bar which allows the respective user to search for other specific users, specific trending topics, and specific Tweets the user might be interested in. While using Twitter, users also view various types of advertisements, which are paid for by advertisers and generate billions of dollars for Twitter.

18. Twitter operates on a so-called freemium model: meaning, it does not cost anything to sign up for and use a Twitter account. Twitter also has a premium model (Twitter Blue) which allows certain Twitter users to gain access to components of the platform that are otherwise inaccessible to free Twitter users.

19. Upon signing up for a Twitter account, all users must agree to the Terms of Service, which incorporates the Twitter Privacy Policy.

20. Twitter's Privacy Policy describes how Twitter uses the information that it collects from users, inclusive of the PII collected from Twitter users when they initially sign up to use Twitter. At no point does Twitter disclose in their Privacy Policy that they allow cybercriminals to commandeer Twitter's API in order to scrape sensitive PII from Twitter and to then weaponize or sell that information on the dark web. Indeed, Twitter categorizes their use of PII into the following use-categories: (1) to operate, improve, and personalize services, (2) to foster safety and security, (3) to measure, analyze and make [Twitter's] services better, (4) to communicate with [Twitter users] about [Twitter's] services, and (5) for research purposes. None of these use categories discuss or give permission to Twitter to publicly expose user PII to cybercriminals.

21. Notably, the Privacy Policy does contemplate sharing PII with third parties in certain limited circumstances through Twitter's APIs. The privacy policy states:

> We use technology like APIs and embeds to make public Twitter information available to websites, apps, and others for their use, for example, displaying Tweets on a news website or analyzing what people say on Twitter. We generally make this content available in limited quantities for free and charge licensing fees for large-scale access. We have standard terms that govern how this information can be used, and a compliance program to enforce these terms. But these individuals and companies are not affiliated with Twitter, and their offerings may not reflect updates you make on Twitter. For more information about how we make public data on Twitter available to the world, visit https://developer.twitter.com.

22. Within Twitter's Privacy Center – an almost unreadable labyrinth of information stored on Twitter's website which contains the Privacy Policy – Twitter states, "[y]out have more control over your Twitter experience than you might think."

23. Regrettably, as Plaintiff Gerber and members of the Class would or will soon find out, this representation is false.

Defendant's API Exploitation

24. From at least on or about June 2021 through on or about January 2022, a defect in Twitter's API allowed cybercriminals to exploit this defect and "scrape" data from Twitter. Specifically, the information compromised included Twitter usernames in combination with email addresses and phone numbers associated with specific Twitter accounts. This has and had the effect of deanonymizing Twitter users (like Plaintiff and members of the putative Class) who had wished to stay anonymous while using Twitter.

25. Twitter stated publicly in 2022 that this API exploitation would not harm Twitter's users, stating in relevant part: "[w]hen we learned about this, we immediately investigated and fixed it. At that time, we had no evidence to suggest someone had taken advantage of the vulnerability." This statement is highly problematic because it evidences that Twitter, which to this day has failed to notify or contact the victims of this particular API exploitation, fails to appreciate the seriousness of what has occurred or take proper steps to attempt to remediate, in any way, the damage caused to its users.

26. The PII belonging to victims of the API exploitation is now being disseminated and sold on the dark web by cybercriminals who mined the information, despite Twitter's representations and omissions to the contrary.

Twitter's 2011 Agreement with the Federal Trade Commission

27. In 2011, Twitter and the FTC entered into an agreement in response to Twitter's alleged violations of Section 5(a) of the FTC Act for misrepresenting the extent to which it protected consumers' privacy. The Agreement (which was ultimately memorialized in a consent order) prohibited Twitter from using "any telephone number or email address obtained from a [u]ser before the effective date of this Order for the purpose of enabling an account security feature." While the Agreement did not prohibit Twitter from doing so in the future, it would first have to comply with notice, disclosure, and consent requirements of the Agreement.

28. The Agreement and consent order prohibits Twitter from misrepresenting "the extent to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, including, but not limited to, misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users."

29. Twitter's failures with respect to the 2021-2022 API exploitation are a violation of the FTC Agreement and consent order, which were facially designed to benefit Plaintiff and members of the Class and to protect them from the very harm that Twitter would inflict on them.

Harm to Consumers

30. Not only is it always dangerous as a general matter for email addresses and phone numbers to appear on the dark web with respect to how that information might be used, but, given that Twitter's API exploitation allows cybercriminals to link the Twitter persona of a respective user to their PII, this intrusive privacy violation is all the more dangerous and offensive under these unique circumstances.

31. Plaintiff Gerber, like so many tens of millions of Twitter users and putative Class members, accepted Twitter's invitation to stay anonymous during his use of the Twitter platform.

As such, Plaintiff (like many tens of millions of other Twitter users) used a pseudonym as a username and attempted to conceal his identity when using the platform due to a multitude of well-recognized privacy concerns. However, Twitter, in contravention of the Twitter Privacy Policy and in violation of the FTC agreement an order, failed to ensure that Plaintiff Gerber's account would remain anonymous, as was his right (and expectation) when he signed up for Twitter initially.

32. Plaintiff Gerber and the members of the Class suffered significant harm as a result of Twitter's failure to protect their PII. This harm includes: (1) Twitter users being subjected to potential phishing attacks and other types of targeted, email-centric privacy intrusions; (2) Twitter users being subject to potential unwanted robocalls and texts and other types of targeted, phone-centric privacy intrusions; (3) Twitter users having private Twitter accounts unmasked, leading to harm for the multitude of Twitter users who did not wish to have their accounts exposed; (4) Twitter users' loss of time and effort due to the issues caused by having their private Twitter accounts unmasked; (5) Twitter users having their PII disseminated and available for sale on the dark web; and (6) perhaps most significantly, the constant and relentless concern that numerous viewpoints and personal information shared anonymously (in some cases regarding a user's most intimate views and matters) over the course of years will now be publicly unmasked as belonging to that particular Twitter user. There is a very concrete harm suffered by the tens of millions of anonymous Twitter users who did not want their actual identities (and, potentially, intimate personal details) revealed to the public. However, against their will, and contrary to the representations made by Twitter, this is exactly what happened.

CLASS ALLEGATIONS

33. Plaintiff brings this nationwide class action pursuant to Rule 23(b) and 23(c) of the Federal Rules of Civil Procedure, on behalf of himself and on behalf of all members of the following class:

> **Nationwide Class.** All Twitter users who had their email addresses and/or telephone numbers compromised by Twitter's API exploitation between June of 2021 through January of 2022 (the "Class").

34. Excluded from the Class are the following individuals and/or entities: Defendant and its parent(s), subsidiaries, affiliate(s), officers and directors, current or former employees, and any entity in which the Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol to opt out; and any and all government officials as well as all judges (and their immediate family members) assigned to this Action.

35. Plaintiff reserves the right to modify or amend the definitions of the proposed Class prior to the Court's determination regarding whether class certification is appropriate.

36. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. Defendant collected the PII of tens of millions of users upon sign up, and that information was compromised by the Twitter API exploitation as described herein. Determining membership in the Class can be easily determined via Defendant's records.

37. **Commonality.** The Class has questions of law and fact that exist which are common among Class members; and these questions of law and fact predominate over any questions affecting only individual Class members. These questions include:

a. Whether Defendant owed a duty to the Class to protect PII;

b. Whether Defendant breached that duty;

c. Whether Defendant violated either its Terms of Service or its Privacy Policy when it allowed the Twitter API exploitation to take place (and, subsequently, when it failed to inform Twitter's users about the exploitation);

d. Whether Defendant's conduct violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. 45(a);

e. Whether Defendant's conduct as alleged herein violates the 2011 FTC Agreement and accompanying consent order;

f. Whether Defendant's conduct violated the state laws as alleged herein;

g. Whether Defendant caused Plaintiff and Class Members' injuries; and

h. Whether Plaintiff and the other Class Members are entitled to monetary, equitable, injunctive, and other appropriate relief.

38. **Typicality.** Plaintiff's claims are typical of those of the other Class Members, all of whom suffered from the Twitter API exploitation's exposure of their PII as alleged herein.

39. **Adequacy**. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff's counsel is competent and is experienced in litigating data breach and privacy-related class action litigations.

40. **Superiority and Manageability**: Under Rule 23(b), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class Members are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished and unrectified. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

41. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final monetary and/or injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of the Plaintiff and the Class)

42. Plaintiff realleges and incorporates by reference the allegations contained in the preceding and following paragraphs.

43. As a condition for doing business, Defendant's current and former consumers were obligated to provide Defendant with the sensitive PII described herein in order to become users of Defendant's platform.

44. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information and/or not disclose their PII to unauthorized third parties or make it publicly available.

45. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

46. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

47. Defendant had a duty to Plaintiff and the class to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

48. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

49. Defendant's duty to use reasonable security measures arose because of the relationship that existed between Defendant and Plaintiff and the Class.

50. Defendant was also subject to an independent duty, untethered to any contract between Defendant and Plaintiff or the Class to safeguard the PII that it solicited and maintained.

51. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

52. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII stored on Defendant's systems. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the API exploitation as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the PII of Plaintiff and the Class.

53. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

54. Defendant was able to protect against the harm suffered by Plaintiff and the Class as a result of the API exploitation.

55. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

56. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the API exploitation.

57. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry standard protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

58. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the API exploitation.

59. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

60. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent improper disclosure and dissemination of PII in its possession.

61. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the API exploitation.

62. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

63. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

64. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

65. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that could result to Plaintiff and the Class.

66. Defendant's violation of Section 5 of the FTC Act, as well as the standards of conduct established by these statutes and regulations, constitutes negligence *per se*.

67. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

68. The harm that occurred because of the API exploitation is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, including against Defendant, which (because of its failure to employ reasonable data security measures and avoid unfair and deceptive practices) caused the same harm as that suffered by Plaintiff and the Class.

69. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) potential or actual identity theft; (ii) the loss of the opportunity of (and control over) how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) potential or actual out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the API exploitation; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (vii) costs in terms of time, effort, and money that will (or might) be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the API exploitation for the remainder of the lives of Plaintiff and the Class.

70. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, loss of privacy, and other economic and non-economic losses.

71. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

72. Plaintiff and Class Members are therefore entitled to damages, including actual and compensatory damages, restitution, declaratory and injunctive relief, and attorney's fees, costs, and expenses.

COUNT II

Breach of Express Contract

(On Behalf of the Plaintiff and the Class)

73. Plaintiff realleges and incorporates by reference the allegations contained in the preceding and following paragraphs.

74. As a condition of using the Twitter platform, Plaintiff and Class Members were required to and did consent to Twitter's Terms of Service, including its Privacy Policy.

75. In exchange for access, Twitter users consented to and allowed Twitter to collect and use certain of their non-public sensitive information. Twitter's Privacy Policy expressly promised users that certain other information, like the PII of Plaintiff and Class Members at issue herein, would not be disclosed to third parties unless and until users affirmatively consented to the disclosure.

76. In consideration for the use of Twitter's platform, Twitter users also provided their PII and their enormous time and attention. As described above, without users' time and attention, Twitter could not monetize these users and promote its number of active users to advertisers to induce them to spend money on the Twitter platform.

77. Twitter warranted in the Privacy Policy that users would be informed as to how their data is collected and used and that users would be empowered to make informed decisions as to what information they chose to share with Twitter. Twitter violated this provision of its contracts with users by failing to disclose in its security prompts that the email addresses and phone numbers users provided for account security would not be adequately protected.

78. Plaintiff and Class Members fully performed their material obligations under their contracts with Twitter. Twitter breached its contractual duties to Plaintiff and Members of the Class by failing to adhere to their promise that users must affirmatively consent to share their PII

with third parties, and by failing to give users meaningful choice or allow them to make informed decisions as to what information they chose to share and with whom.

79. Additionally, Twitter failed to comply with its promise that PII would only be used in conformity with U.S. law by violating the FTC Act and FTC agreement and consent order.

80. As a direct and proximate result of Twitter's breach of contract, Plaintiff and Class Members surrendered their time and attention and their PII to Twitter and did not receive the level of service that they were promised. Twitter users were deprived of the benefit of the bargain that they struck with Twitter and the PII that they provided to Twitter suffered a diminution in value because of being shared with third parties without their consent or knowledge.

81. As a direct and proximate result of Defendant's breach of contract, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III

Violations of California's Unfair Competition Law ("UCL")

(On Behalf of the Plaintiff and the Class)

82. Plaintiff realleges and incorporates by reference the allegations contained in the preceding and following paragraphs.

83. Defendant is a business as defined by the statute.

84. By reason of the conduct alleged herein, Defendant engaged in unlawful "business practices" within the meaning of the UCL.

85. Defendant misrepresented and omitted material information regarding the privacy practices and policies with respect to protecting Twitter users' PII.

86. Defendant did not disclose to Plaintiff and Class Members that the PII that they provided in response to Twitter's representations regarding login verification and account security would not be adequately protected and would be disclosed to unknown third parties.

87. **Unlawful Prong.** Defendant violated the unlawful prong of the UCL because Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

88. Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC §45) prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC Act prohibits acts or practices that cause or are likely to cause substantial injury to consumers, that cannot be reasonably avoided by consumers, and are not outweighed by the countervailing benefits to consumers or the marketplace. The FTC Act also prohibits material representations, omissions, or practices that are likely to mislead reasonable consumers. This prohibition applies to all persons engaged in commerce, including Defendant.

89. Plaintiff and Class Members are consumers within the meaning of the FTC Act and Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect. The harm that occurred as alleged herein is the type of harm that the FTC Act was intended to guard against.

90. Twitter's failure to protect the PII of Plaintiff and Class Members, is an unfair and deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

91. Moreover, Twitter's violation of the 2011 FTC agreement and consent order is a violation of the unlawful prong of the UCL. The agreement and consent order prohibited Twitter from engaging in the exact conduct as alleged herein and was intended and implemented for the benefit of Twitter's users and the consumer marketplace. Twitter disregarded these strictures to the detriment of Plaintiff and the Class.

92. Additionally, Twitter violated the unlawful prong of the UCL by violating Cal. Bus. & Prof. Code § 22576, which prohibits Twitter from knowingly, negligently, and materially failing to adhere to its published Privacy Policy. Twitter's Privacy Policy represented that its users would have control over their privacy choices, must affirmatively opt-in to share that information and that email addresses and phone numbers would not be shared with unauthorized third parties.

93. **Unfairness Prong.** The UCL further prohibits unfair acts and practices. Defendant engaged in unfair acts and practices with respect to the collection of PII by failing to fully disclose that it would not be adequately protected. This information was not available to Plaintiff, Class Members, or the public at large. Additionally, Twitter stated that the API exploitation did not result in the exposure of PII, which hamstrung Twitter's users and victims of the exploitation from being able to protect themselves after the exploitation (and subsequent posting of the information on the dark web) had taken place.

94. Due to Defendant's affirmative misrepresentations and material omissions the injury suffered by consumers was not reasonably avoidable through ordinary investigation. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

95. As a result of Defendant's material misrepresentations and omissions which were intended to and did induce Plaintiff and Class Members to surrender their PII to Defendant, Plaintiff and Class Members were harmed and suffered an economic loss. Plaintiff and Class Members lost money and/or property as a result of Defendant's inducements in that they provided valuable, non-public and sensitive contact information and their time and attention to Twitter. This is information and attention for which there is an active and viable marketplace, and the data has a quantifiable value. Plaintiff has also suffered harm in the form of diminution of the value of their non-public and sensitive personally identifiable data.

96. As a result of Defendant's unlawful, unfair, and fraudulent business practices, Plaintiff and Class Members are entitled to relief including restitution and all other remedies allowed by law.

PRAYER FOR RELIEF

97. **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from continuing to refuse to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and

internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and security checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves; and

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

98. Plaintiff hereby demands a trial by jury.

DATED: January 13, 2023

Respectfully submitted,

/s/ Israel David

Israel David*
israel.david@davidllc.com
Blake Hunter Yagman*
blake.yagman@davidllc.com
Hayley Elizabeth Lowe*
hayley.lowe@davidllc.com
Madeline Sheffield*
madeline.sheffield@davidllc.com
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, New York 10004

Tel.: (212) 739-0622

*Pro Hac Vice Forthcoming

Jeff Westerman (Calif. Bar 94559)
jwesterman@jswlegal.com
WESTERMAN LAW CORP.
16133 Ventura Blvd., Suite 685
Encino, California Ca. 91436
Tel.: (310) 698-7450

Attorneys for Plaintiff and the Proposed Class