

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

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

6 *Pro Hac Vice Forthcoming

7 *Attorneys for Plaintiff Gerber*

Local Counsel for Plaintiff Gerber

8 **UNITED STATES DISTRICT COURT**
9 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

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

12
13 Plaintiff,

14 v.

15 TWITTER, INC.;

16
17 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

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

6 **NATURE OF THE ACTION**

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

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

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

24 4. Twitter is obligated, and has promised to, protect certain private information
25 entrusted to it by its users in order to access the platform and, in turn, provide Twitter with the
26 source of its billions in revenues. However, from June 2021 through January 2022, a defect in
27 Twitter’s application programming interface (“API”) allowed cybercriminals to exploit this defect
28

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

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

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

22 6. The cache of information exposed by the API exploitation includes over
23 200,000,000 Twitter users’ information including the aforementioned PII. Because of the
24 anonymized, pseudo-anonymized and confidential nature of Twitter (which, as detailed above, is
25 Twitter’s core premise and value proposition to would-be users), these Twitter users were not only
26

27 _____
28 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...”

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

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

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

18 **JURISDICTION AND VENUE**

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

26 10. This Court has personal jurisdiction over the Defendant because Defendant
27 maintains its principal place of business in this District, at 1355 Market Street, San Francisco,
28

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

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

7 **PARTIES**

8 ***Plaintiff Stephen Gerber***

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

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

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

21 ***Defendant Twitter, Inc.***

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

25 **FACTUAL ALLEGATIONS**

26 ***Defendant's Business and Privacy Policy***

27 16. Twitter operates one of the largest social media platforms in the world.
28

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

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

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

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

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

1
2 We use technology like APIs and embeds to make public Twitter
3 information available to websites, apps, and others for their use, for
4 example, displaying Tweets on a news website or analyzing what people
5 say on Twitter. We generally make this content available in limited
6 quantities for free and charge licensing fees for large-scale access. We
7 have **standard terms** that govern how this information can be used, and a
8 compliance program to enforce these terms. But these individuals and
9 companies are not affiliated with Twitter, and their offerings may not reflect
10 updates you make on Twitter. For more information about how we make
11 public data on Twitter available to the world,
12 visit <https://developer.twitter.com>.

9 22. Within Twitter’s Privacy Center – an almost unreadable labyrinth of information
10 stored on Twitter’s website which contains the Privacy Policy – Twitter states, “[y]ou have more
11 control over your Twitter experience than you might think.”

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

14 ***Defendant’s API Exploitation***

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

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

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

4 ***Twitter’s 2011 Agreement with the Federal Trade Commission***

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

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

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

20 ***Harm to Consumers***

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

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

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

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

22 CLASS ALLEGATIONS

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

26
27 **Nationwide Class.** All Twitter users who had their email addresses and/or
28 telephone numbers compromised by Twitter's API exploitation between June of
2021 through January of 2022 (the "Class").

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

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

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

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

20 **CAUSES OF ACTION**

21 **COUNT I**

22 **Negligence**

23 **(On Behalf of the Plaintiff and the Class)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13 **COUNT III**

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

15 **(On Behalf of the Plaintiff and the Class)**

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

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

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

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

23 86. Defendant did not disclose to Plaintiff and Class Members that the PII that they
24 provided in response to Twitter's representations regarding login verification and account security
25 would not be adequately protected and would be disclosed to unknown third parties.
26
27
28

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

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

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

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

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

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

- 1 A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his
2 Counsel to represent the Class;
- 3 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
4 complained of herein pertaining to the misuse and/or disclosure of the PII of
5 Plaintiff and Class Members, and from continuing to refuse to issue prompt,
6 complete, and accurate disclosures to Plaintiff and Class Members;
- 7 C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive
8 and other equitable relief as is necessary to protect the interests of Plaintiff and
9 Class Members, including but not limited to an order:
- 10 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
11 described herein;
- 12 ii. requiring Defendant to protect, including through encryption, all data collected
13 through the course of its business in accordance with all applicable regulations,
14 industry standards, and federal, state or local laws;
- 15 iii. requiring Defendant to delete, destroy, and purge the personal identifying
16 information of Plaintiff and Class Members unless Defendant can provide to
17 the Court reasonable justification for the retention and use of such information
18 when weighed against the privacy interests of Plaintiff and Class Members;
- 19 iv. requiring Defendant to implement and maintain a comprehensive Information
20 Security Program designed to protect the confidentiality and integrity of the PII
21 of Plaintiff and Class Members;
- 22 v. requiring Defendant to engage independent third-party security
23 auditors/penetration testers as well as internal security personnel to conduct
24 testing, including simulated attacks, penetration tests, and audits on
25 Defendant's systems on a periodic basis, and ordering Defendant to promptly
26 correct any problems or issues detected by such third-party security auditors;
- 27 vi. requiring Defendant to engage independent third-party security auditors and
28

- 1 internal personnel to run automated security monitoring;
- 2 vii. requiring Defendant to audit, test, and train its security personnel regarding any
- 3 new or modified procedures;
- 4 viii. requiring Defendant to segment data by, among other things, creating firewalls
- 5 and access controls so that if one area of Defendant's network is compromised,
- 6 hackers cannot gain access to other portions of Defendant's systems;
- 7 ix. requiring Defendant to conduct regular database scanning and security checks;
- 8 x. requiring Defendant to establish an information security training program that
- 9 includes at least annual information security training for all employees, with
- 10 additional training to be provided as appropriate based upon the employees'
- 11 respective responsibilities with handling personal identifying information, as
- 12 well as protecting the personal identifying information of Plaintiff and Class
- 13 Members;
- 14 xi. requiring Defendant to routinely and continually conduct internal training and
- 15 education, and on an annual basis to inform internal security personnel how to
- 16 identify and contain a breach when it occurs and what to do in response to a
- 17 breach;
- 18 xii. requiring Defendant to implement a system of tests to assess its employees'
- 19 knowledge of the education programs discussed in the preceding
- 20 subparagraphs, as well as randomly and periodically testing employees'
- 21 compliance with Defendant's policies, programs, and systems for protecting
- 22 personal identifying information;
- 23 xiii. requiring Defendant to implement, maintain, regularly review, and revise as
- 24 necessary a threat management program designed to appropriately monitor
- 25 Defendant's information networks for threats, both internal and external, and
- 26 assess whether monitoring tools are appropriately configured, tested, and
- 27 updated;
- 28

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28