Sophia M. Rios (SBN 305801
BERGER MONTAGUE PC
401 B street, Suite 2000
San Diego, CA 92101
Telephone: (619) 489-0300
srios@bm.net

John A. Yanchunis
(*pro hac vice* forthcoming)
Jean Sutton Martin
(*pro hac vice* forthcoming)
Patrick Barthle
(*pro hac vice* forthcoming)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jyanchunis@ForThePeople.com
jeanmartin@ForThePeople.com
pbarthle@ForThePeople.com

Counsel for Plaintiff and the Proposed Class

Additional counsel on signature page.

CGC-23-605100

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

Henry Yeh, individually and on behalf of all others similarly situated,

Plaintiff,

v.

Twitter, Inc.,

Defendant.

CASE NO.:

CLASS ACTION COMPLAINT for:

1. **Breach of Contract**
2. **Breach of Implied Contract**
3. **Violations of Business and Professions Code § 17200, et seq.**
4. **Unjust Enrichment**

DEMAND FOR JURY TRIAL

Plaintiff Henry Yeh, individually and on behalf of all others similarly situated, files this Class Action Complaint against defendant Twitter, Inc. ("Twitter" or "Defendant"), and in support states the following.

INTRODUCTION

1. Twitter operates an online communication service through its website, www.twitter.com, and through text messaging and mobile applications. The service allows registered users to communicate with one another by posting "tweets," or short messages currently limited to 280 characters or less, with which other users may interact through a "like," reply, or "retweet."

2. In order to follow other accounts, or post, like, and retweet tweets, users must register for a Twitter account.

3. This lawsuit concerns Twitter's surreptitious and undisclosed use of Plaintiff's and Class Members' telephone numbers and email addresses (hereinafter "Personal Information") for advertising and marketing purposes, and, ultimately, its own unjust enrichment.

4. Twitter solicited and collected Plaintiff's and Class Members' telephone numbers and email addresses under the guise that they were to be used for various account security related functions, including two-factor authentication, account recovery, and account re-authentication, as further described below.

5. In reality, Twitter was also using this Personal Information of Plaintiff and Class Members to line its own pockets—specifically, it utilized the provided telephone numbers and email addresses in its "Tailored Audiences" and "Partner Audiences" marketing products, thereby permitting advertisers to target specific groups of Twitter users by matching the telephone numbers and email addresses that Twitter collected to the advertisers' existing (or purchased) lists of telephone numbers and email addresses.

6. On May 25, 2022, the Attorney General by the Federal Trade Commission ("FTC" or "Commission") filed a complaint concerning this conduct and likewise announced that Twitter will pay a $150 million fine to settle the allegations. *See United States of America v. Twitter, Inc.*, Case No. 3:22-cv-3070. ECF. No. 1 (N.D. Cal.) ("2022 FTC Complaint"); Federal Trade Comm.

Twitter to pay $150 million penalty for allegedly breaking its privacy promises – again (May 25, 2022), *available at* https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again.

7. This case seeks vindication and recompense on behalf of the individual consumers whose Personal Information Twitter connivingly collected and deployed.

THE PARTIES

8. Plaintiff Henry Yeh is an adult domiciled in South San Francisco, California. He has an active Twitter account and had an active Twitter account during the entire Class Period.

9. Plaintiff Henry Yeh is a Twitter user who between May 2013 and September 2019 provided his telephone number and email address to Twitter for the purposes of login verification and account recovery. He brings claims on behalf of himself and other similarly-situated Twitter users in California (the "Class" defined in paragraph 99; the members of the Class are referred to as "Class Members") arising from Twitter's knowing, unauthorized, and undisclosed use of their Personal Information for advertising and/or marketing purposes.

10. Plaintiff Henry Yeh valued his telephone number and email address and would not have provided them without receiving value in exchange had he known this Personal Information would be used for marketing purposes, rather than solely for the login verification and account recovery purposes Twitter touted.

11. Twitter is a Delaware corporation with its principal place of business at 1355 Market Street, Suite 900, San Francisco, California, 94103. Twitter transacts or has transacted business in this County and throughout the State of California and the United States. At all times material to this Complaint, Twitter has operated its online communication service through its website, www.twitter.com, and through its mobile applications.

JURISDICTION AND VENUE

12. This Court has personal jurisdiction over Defendant because Twitter's principal place of business is in California and this County. Additionally, Defendant is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's and Class Members' claims occurred in this State.

13. Defendant conducts substantial business in the State of California and this County. Defendant has sufficient minimum contacts with and/or otherwise intentionally avails itself of the markets in the State of California and this County, and has sufficient contacts with the State of California and this County such that it is fair and just for Defendant to adjudicate this dispute here in this County and in the State of California.

14. This Court has subject matter jurisdiction over this entire action because the matter in controversy, exclusive of interest and costs, exceeds the jurisdictional minimum of the Court. The acts and omission complained of in this action took place in the State of California.

15. Venue is proper because this is a class action, and the acts and/or omissions complained of took place, in whole or in part, within the venue of this Court. Defendant conducts business in this County, and a substantial amount of Defendant's wrongdoing is believed to have occurred in this County. In addition, a significant number of Class Members reside in this County and in the State of California.

FACTUAL ALLEGATIONS CONCERNING TWITTER

I. Twitter's History of Privacy Violations & Its Agreement with the FTC

16. Twitter's violation of consumers' privacy rights is not new – it has been persistent and pervasive for at least a decade.

17. In 2011, the FTC charged Twitter with engaging in deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), for its failures to provide reasonable security measures to prevent unauthorized access to nonpublic user information and to honor the privacy choices exercised by Twitter users. *See*, *In re Twitter, Inc*., C-4316, 151 F.T.C. 162 (Mar. 11, 2011) ("Administrative Complaint") ¶¶ 13-17.[1]

18. Specifically, the Administrative Complaint asserted that Twitter had engaged in deceptive acts or practices by misrepresenting that users could control who had access to their tweets through a "protected account" or could send private "direct messages" that could only be viewed by the recipient when, in fact, Twitter lacked reasonable safeguards to ensure those choices

[1] The 2011 Administrative Complaint is also available at: https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf (last visited Feb. 24, 2023).

were honored, such as restricting employee access to nonpublic user information based on a person's job requirements. *See* Administrative Complaint ¶¶ 6, 11-12.

19. The Administrative Complaint also alleged that Twitter had misrepresented the controls it implemented to keep user accounts secure, when, in fact, Twitter lacked reasonable safeguards to limit or prevent unauthorized access to nonpublic user information, such as secure password requirements and other administrative, technical, or physical safeguards. *See* Administrative Complaint ¶¶ 10-12.

20. Twitter entered a consent settlement to resolve the Commission's Administrative Complaint for alleged violations of Section 5(a) of the FTC Act which was memorialized in a 2011 order issued by the FTC. *See In re Twitter, Inc.*, C-4316, 151 F.T.C. 162 (Mar. 11, 2011) (Decision and Order) ("Commission Order" or "2011 Order").[2] The Commission Order became final in March 2011 and remains in effect. *See* Commission Order, Provision VIII.

21. Provision I of the Commission Order, in relevant part, states:

> **IT IS ORDERED that respondent**, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, **shall not misrepresent in any manner, expressly or by implication, the extent to which respondent 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**.

See Commission Order, Provision I (emphasis added). The Commission Order required Twitter to refrain from such misrepresentations for a period of 20 years from the date of the Order (at least March 2, 2031). *See* Commission Order, Provision VIII.

22. Importantly, the Commission Order defines "nonpublic consumer information" as, in relevant part, "an individual consumer's: (a) email address... [and] (c) mobile telephone number[.]" *See* Commission Order, Definition 3.

[2] The 2011 Commission Order is also available at: https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf (last visited Feb. 24, 2023).

II. Twitter Misrepresented the Purposes for Which it Collected Plaintiff's and Class Members' Telephone Numbers and Email Addresses

23. Twitter's platform is widely used. As of September 2019, Twitter had more than 330 million monthly active users worldwide, which included journalists, celebrities, commercial brands, and government officials.

24. Commercial entities regularly use Twitter to advertise to consumers. Indeed, Twitter's core business model monetizes user information by using it for advertising. In fact, of the $3.4 billion in revenue that Twitter earned in 2019, $2.99 billion flowed from advertising.

25. Twitter primarily allows companies to advertise on its service through "Promoted Products," which can take one of three forms: (1) Promoted Tweets, which appear within a user's timeline, search results, or profile pages, similar to an ordinary tweet; (2) Promoted Accounts, which typically appear in the same format and place as other recommended accounts; and (3) Promoted Trends, which appear at the top of the list of trending topics for an entire day.

26. Twitter offers various services that advertisers can use to reach their existing marketing lists on Twitter, including "Tailored Audiences" and "Partner Audiences." Tailored Audiences allows advertisers to target specific groups of Twitter users by matching the telephone numbers and email addresses that Twitter collects to the advertisers' existing lists of telephone numbers and email addresses. Partner Audiences allows advertisers to import marketing lists from data brokers like Acxiom and Datalogix to match against the telephone numbers and email addresses collected by Twitter. Twitter has provided advertisers the ability to match against lists of email addresses since January 2014 and against lists of telephone numbers since September 2014.

27. Twitter has prompted users to provide a telephone number or email address for the express purpose of securing or authenticating their Twitter accounts. However, through at least September 2019, Twitter also used this information to serve targeted advertising and further its own business interests through its Tailored Audiences and Partner Audiences services. For example, from at least May 2013 until at least September 2019, Twitter collected telephone numbers and email addresses from users specifically for purposes of allowing users to enable two-factor authentication, to assist with account recovery (e.g., to provide access to accounts when users have

forgotten their passwords), and to re-authenticate users (e.g., to re-enable full access to an account after Twitter has detected suspicious or malicious activity). From at least May 2013 through at least September 2019, Twitter did not disclose, or did not disclose adequately, that it used these telephone numbers and email addresses to target advertisements to those users through its Tailored Audiences and Partner Audiences services.

28. As noted above, the 2011 Commission Order, among other things, prohibited Twitter from misrepresenting the extent to which Twitter maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information.

29. Yet, from at least May 2013 until at least September 2019, Twitter misrepresented to users of its online communication service the extent to which it maintained and protected the security and privacy of their Personal Information. Specifically, while Twitter represented to users that it collected their telephone numbers and email addresses to secure their accounts, Twitter failed to disclose that it also used user's Personal Information to aid advertisers in reaching their preferred audiences. Twitter's misrepresentations violate the FTC Act and the 2011 Order, which specifically prohibited the company from making misrepresentations regarding the security of nonpublic consumer information like the Personal Information.

30. According to the 2022 FTC Complaint, more than 140 million Twitter users provided email addresses or telephone numbers to Twitter based on Twitter's deceptive statements that their information would be used for specific purposes related to account security. Twitter knew or should have known that its conduct violated the 2011 Order, which prohibits misrepresentations concerning how Twitter maintains email addresses and telephone numbers collected from users.

31. Technology companies like Twitter recognize the monetary value of users' Personal Information, insofar as they encourage users to install applications explicitly for the purpose of selling that information to technology companies in exchange for monetary benefits.[3]

[3] Kari Paul, *Facebook launches app that will pay users for their data*, The Guardian (June 11, 2019), https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-study (last visited Feb. 22, 2023); Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html (last visited Feb. 22, 2023);; Jay Peters, *Facebook will now pay you for your*

32. Through its deceptive information collection techniques and misrepresentations, Twitter is unjustly enriching itself at the cost of consumer choice, when the consumer would otherwise have the ability to choose whether and how they would monetize their own data.

A. Plaintiff (and Advertisers) Value Email Addresses and Phone Numbers.

33. Plaintiff valued his telephone number and email address and would not have provided them to Twitter without receiving value in exchange had he known this Personal Information would be used for marketing purposes, rather than for the login verification and account recovery purposes Twitter touted.

34. Indeed, numerous marketing services and consultants, offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of Twitter's targeted marketing at issue here—direct putative advertisers to offer consumers something of value in exchange for their personal information:

- "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course, or something else valuable." [4]
- "The first thing you need to do is create an opt in page with a 'free gift' to incentivize Twitter users to join your list. . . . It could be an infographic, audio interview, video, report, or series of emails, but you need to answer the magical question in your prospect's mind: 'What's in it for me?'" [5]
- "Capturing email addresses through . . . campaigns such as welcome offers, cart savers, spin to wins, and other display options – and then sending automated emails to those contacts can be a key driver for growing your online revenue." [6]
- "What most people do when they want to build an email list is to put an optin [sic]

voice recordings, The Verge (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounciations-app (last visited Feb. 22, 2023).

[4] Vero, *How to Collect Emails Addresses on Twitter* (June 2014), available at https://www.getvero.com/resources/twitter-lead-generation-cards/ (last visited Feb. 22, 2023).

[5] Kajabi, *6 Simple Ways To Build Your Email List On Twitter* (last visited Feb. 22, 2023), *available at* https://kajabi.com/blog/6-simple-ways-to-build-your-email-list-on-twitter

[6] Josh Mendelsohn, PRIVY, *How Much an Email Address is Worth to Your Online Business* (July 11, 2022), *available at* https://www.privy.com/blog/whats-the-value-of-an-email-address (last visited Feb. 22, 2023).

form on their website and hope that people sign up. Unfortunately, this strategy usually doesn't work very well. To grow your email list, you need to attract people with a compelling offer. You need a lead magnet. What is a Lead Magnet? A lead magnet (a.k.a. an optin bribe) is something awesome that you give away for free in exchange for an email address." [7]

- "Tempt your customers with a competition to win a cool prize. Remember, the numbers you collect are worth their weight in gold for SMS marketing, so make sure your prize is worth the exchange. . . . Similar to text-to-win competitions, keyword SMS campaigns are about giving your customers a great deal in exchange for their phone number. Run an ad asking them to text you, and you send them a special offer or discount in return. . . . When you're asking for something valuable like a customer's phone number, you need to make it worth their while. What can you give your customers that no one else can?" [8]

35. These marketing companies/consultants have placed varying estimates on the value derived from obtaining such email addresses, indicating increased revenue from each email address of $33,[9] and that "the dollar value [that] each customer [spent] that received email was $625 for the year compared with $113 for each customer that did not receive any email. A customer that received email spent an astonishing 550% more a year with them on average than those that did not."[10] And, while the value to an advertiser of an email address is around $33, the value of a

[7] OptinMonster.com, *Email Marketing: The #1 Ridiculously Easy Way To Grow Your Business* (July 11, 2022), *available at* https://optinmonster.com/beginners-guide-to-email-marketing/(last visited Feb. 22, 2023).

[8] MessageMedia.com, 17 ways to collect your customers' phone numbers for SMS marketing (Nov. 2022), *available at* https://messagemedia.com/us/blog/customer-numbers-sms-marketing/ (last visited Feb. 22, 2023).

[9] Mendelsohn, supra Note 6; *see also, e.g.*, Tara Johnson, TINUITI, *The Rising Value of Email Marketing and First Party Data [in a Cookie-less World]* (March 9, 2021), *available at* https://tinuiti.com/blog/data-privacy/email-marketing-first-party-data/ ("According to Shopify, the value of an email contact rose from $16 in 2019 to $33 in 2020 (and we expect this trend to continue throughout 2021). [ ] Email & mobile numbers will likely become the unique identifier for site users.") (last visited Feb. 22, 2023).

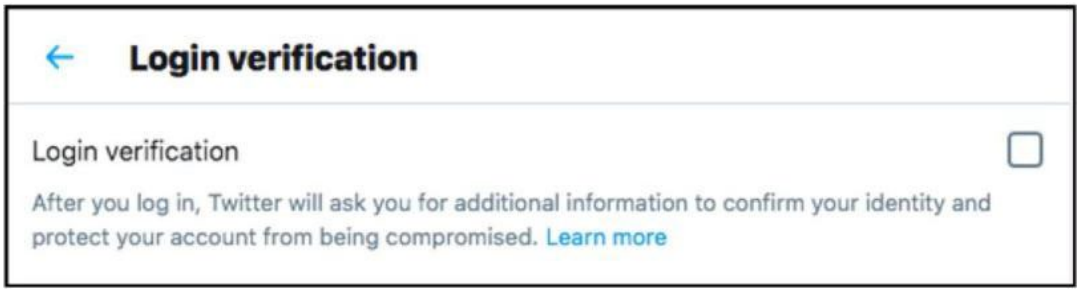
[10] Dela Quist, ONLY INFLUENCERS, Case Study: What is an Email Address Worth and How to Increase Its Value by 176% (last visited Feb. 22, 2023), *available at* https://onlyinfluencers.com/email-marketing-blog-posts/best-practice-email-strategy/entry/case-study-what-is-an-email-address-worth-and-how-to-increase-its-value-by-176

mobile telephone number was multiples higher: $100.87.[11]

36. These various sources make clear that consumers—including the Plaintiff and each Class Member here—value their email addresses and phone numbers and do not give up their contact information for marketing purposes for free; yet that is precisely what Twitter was able to here through deception.

B. Twitter's Deceptive Collection of Personal Information for Two-Factor Authentication

37. Since May 2013, Twitter has allowed users to log into Twitter with two-factor authentication using their telephone numbers. Users who enable this security feature log into their Twitter accounts with their usernames, passwords, and a code texted to their telephone numbers whenever they log in from a new or unrecognized device.



38. Twitter prompts users to enable two-factor authentication through notices on their timelines and after users reset their passwords. Twitter also encourages users to turn on two-factor authentication in tweets from Twitter-operated accounts, Help Center documentation, and blog posts.

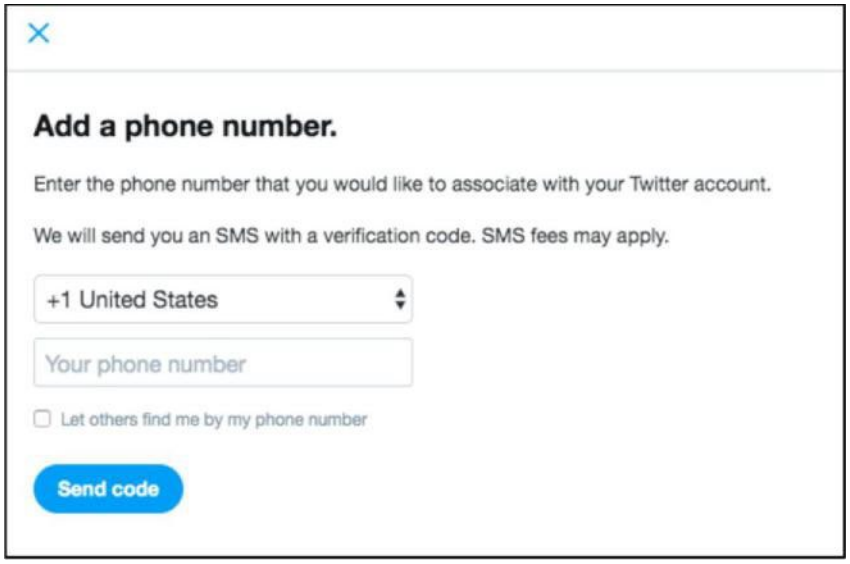
39. To enable two-factor authentication, Twitter users must navigate to an account settings page. After clicking on "Security," users see a screen similar to the one depicted above.

40. When users click on the "Learn more" link, they see a webpage that says, "How to use two-factor authentication." This page states, in relevant part:

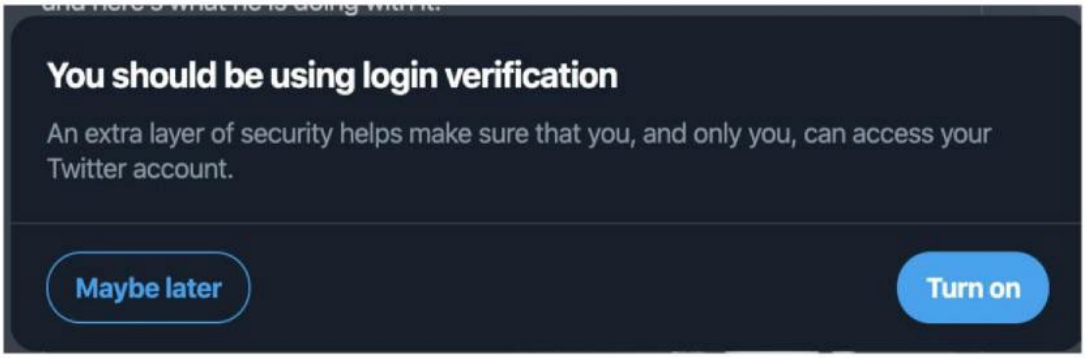
> Two-factor authentication is an extra layer of security for your Twitter account. Instead of only entering a password to log in, you'll also enter a code or use a security key. This additional step helps make sure that you, and only you, can access your account.

[11] AvidMobile.com, *What is a mobile number worth in SMS marketing?* (last visited Feb. 22, 2023), *available* at https://www.avidmobile.com/blog/mobile-number-worth-sms-marketing.php

41. After clicking on the "Login Verification" checkbox above, users see additional instructions about how to enable two-factor authentication. The last screen in the user flow related to two-factor authentication using a telephone number is similar to the one depicted below:



42. Since at least September 2018, Twitter has prompted users to enable two-factor authentication directly on users' timelines through a prompt similar to the screen depicted below:



43. According to the 2022 FTC Complaint, until September 2019, Twitter did not disclose at any point in the two-factor authentication pathway or in any of the associated links described above that it was using the telephone numbers users provided for two-factor authentication to target advertisements to those users.

44. According to the 2022 FTC Complaint, from May 2013, approximately two million users provided a telephone number to enable two-factor authentication.

45. The fact that Twitter used the telephone numbers provided for two-factor authentication for advertising would be material to users when deciding whether to provide a

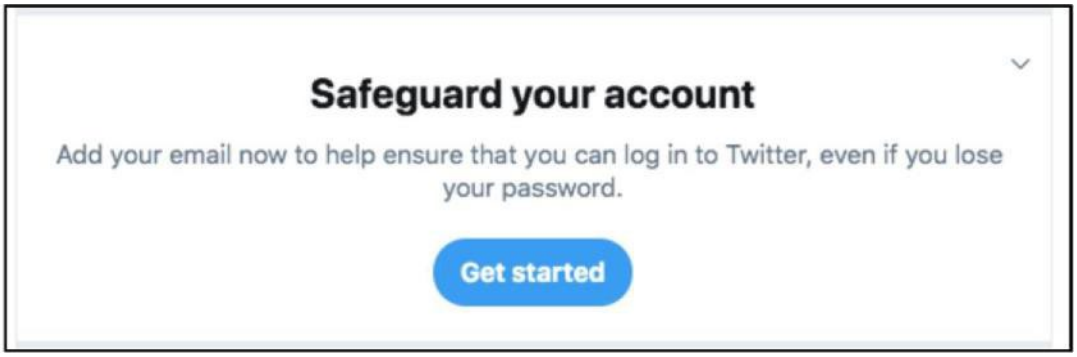
telephone number for two-factor authentication.

C. Twitter's Deceptive Collection of Personal Information for Account Recovery

46. In June 2015, Twitter began prompting users to add a telephone number to their Twitter accounts as a safeguard in the event of a lost password. Then, in April 2018, Twitter also began prompting users to add an email address.

47. Since June 2015, if users do not have a telephone number associated with their accounts, Twitter may prompt the users to add a telephone number through a message similar to the one depicted below:

48. Similarly, since April 2018, if a user does not have an email address associated with their account, Twitter may prompt the user to add an email address through a message similar to the one depicted below:



49. Through September 2019, Twitter did not disclose at any point in the account recovery pathway or any of the messages described above that it was using the telephone numbers or email addresses users provided for account recovery to target advertisements to those users.

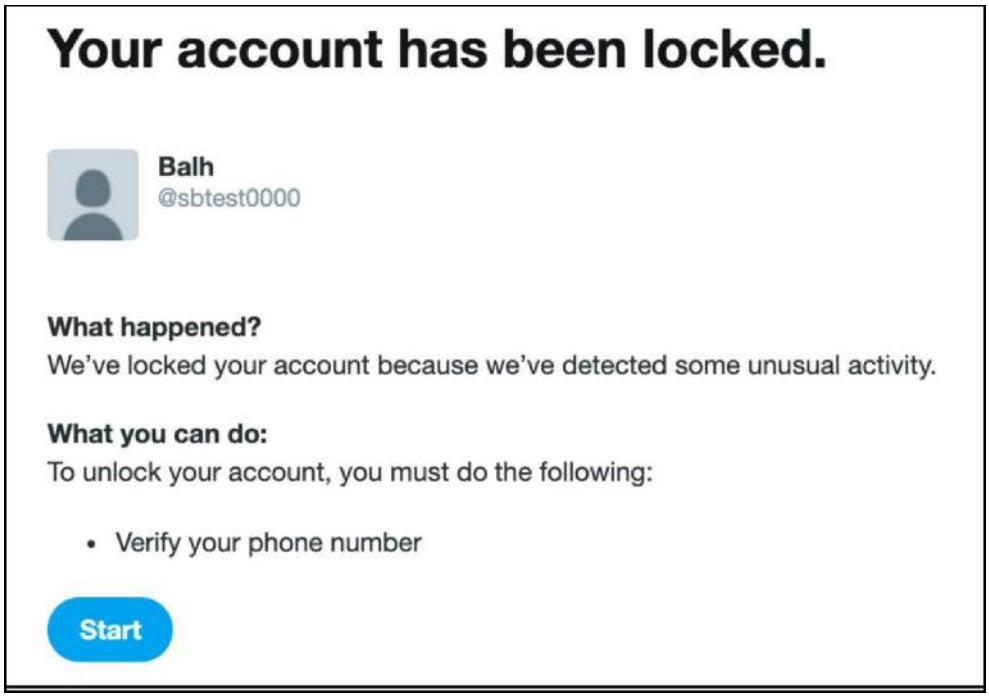
50. According to the 2022 FTC Complaint, from June 2015, approximately 37 million users provided a telephone number or email address for account recovery purposes.

51. The fact that Twitter used the telephone numbers and email addresses provided by users for the purpose of safeguarding their accounts for advertising would be material to users when deciding whether to provide their information for account recovery purposes.

D. Twitter's Deceptive Collection of Personal Information for Re-Authentication

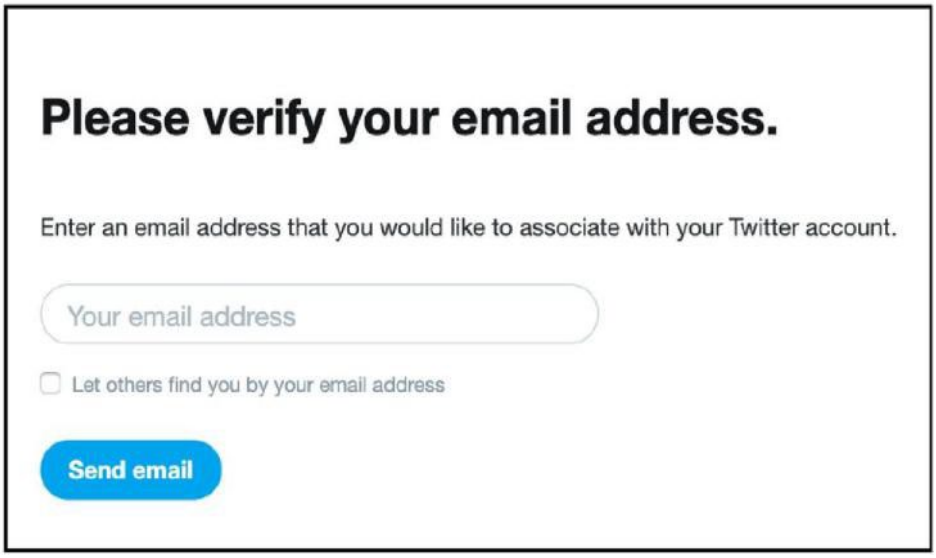
52. In December 2013, Twitter began requiring users to provide a telephone number or email address for re-authentication (e.g., to re-enable full access to an account after Twitter has detected suspicious or malicious activity).

53. If Twitter detects suspicious or malicious activity on a user's account, or suspects that the account may belong to a previously banned user, Twitter may require the user to re-authenticate by providing a telephone number through a prompt similar to the one depicted below:



54. If users click the "Start" button pictured above, they are instructed to enter a telephone number through a prompt similar to the one depicted below:

Similarly, Twitter may require users to provide an email address to re-enable full access to their accounts with a prompt similar to the one depicted below:



55. Through September 2019, Twitter did not disclose at any point in the re-authentication pathway described above that it was using the telephone numbers or email addresses users provided for re-authentication to target advertisements to those users.

56. According to the 2022 FTC Complaint, from September 2014, approximately 104 million users provided a telephone number or email address in response to a prompt for re-authentication.

57. The fact that Twitter used the telephone numbers and email addresses provided for

re-authentication for advertising would be material to users when deciding whether to provide their information in response to a prompt for re-authentication.

III. Twitter Misrepresented that it Processed Personal Data in Accordance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

58. The European Union and Switzerland have each established regulatory regimes to protect individuals' right to privacy with respect to the processing of their personal data. Both privacy regimes generally prohibit businesses from transferring personal data to third countries unless the recipient jurisdiction's laws are deemed to adequately protect personal data.

59. To ensure adequate privacy protections for commercial data transfers, the International Trade Administration of the U.S. Department of Commerce ("Commerce") coordinated with the European Commission and the Swiss Administration to craft the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("Privacy Shield" or "Frameworks"). The Frameworks are materially identical.

60. To rely on the Privacy Shield for data transfers, a company needed to self-certify and annually affirm to Commerce that it complied with the Privacy Shield Principles (the "Principles"). Of note, Principle 5(a) provided that "[a]n organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual." The Frameworks defined "processing" to include "any operation or set of operations which is performed upon personal data, whether or not by automated means" and includes, among other things, "collection," "storage," and "use" of personal information.

61. Companies under the enforcement jurisdiction of the FTC, as well as the U.S. Department of Transportation, were eligible to join the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. A company under the FTC's jurisdiction that self-certified to the Privacy Shield Principles, but failed to comply with the Privacy Shield, may be subject to an enforcement action based on the FTC's deception authority under Section 5 of the FTC Act.

62. Commerce maintains a public website, https://www.privacyshield.gov, where it posts the names of companies that have self-certified to the Privacy Shield. The listing of

companies, found at https://www.privacyshield.gov/list, indicates whether the company's self-certification is current.

63. On November 16, 2016, Twitter self-certified its participation in the Privacy Shield. Twitter has reaffirmed its participation in the Privacy Shield to Commerce each year thereafter.

64. As described above, through at least September 2019, Twitter deceptively used Personal Information collected for specific security-related purposes for advertising.

65. Twitter's use of such Personal Information for advertising purposes was not compatible with the purposes for which the information was collected, and Twitter did not obtain subsequent authorization from any individual to use such information for advertising.

66. As a company under the jurisdiction of the FTC, Twitter's failure to comply with the Privacy Shield, is a violation of Section 5 of the FTC Act.

IV. Twitter Violated Its Privacy Policy and Cal. Bus. & Prof. Code § 22576

67. Pursuant to its Terms of Service, Twitter's Privacy Policy (https://www.twitter.com/privacy) "describes how we handle the information you provide to us when you use our Services. You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information . . ."[12]

68. Twitter's Privacy Policy—as set out at https://twitter.com/en/privacy/previous[13]—repeatedly touts how it respects its users' privacy and does not disclose users' information without their consent.

69. For example, it states:

- "We believe you should always know what data we collect from you and how we use it, and that you should have meaningful control over both. We want to empower

[12] Twitter Terms of Service, effective May 25, 2018, at § 2, *available at* https://twitter.com/en/tos/previous/version_13. Prior versions of the Terms of Service are virtually identical in this respect. *See, e.g.*, Twitter Terms of Service, effective June 25, 2012, at § 2, *available at* https://twitter.com/en/tos/previous/version_7 ("Any information that you provide to Twitter is subject to our Privacy Policy, which governs our collection and use of your information. You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information . . ..")

[13] As noted above, the conduct at issue here occurred between December 2013 and September 2019, and thus it is the versions of the Terms of Service and Privacy Policy effective during that timeframe that are applicable here. For purposes of brevity, Plaintiff quotes here the language of the versions effective in 2018.

you to make the best decisions about the information that you share with us." Privacy Policy, effective May 25, 2018, p. 1, *available at* https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-page-gdpr/pdfs/PP_Q22018_April_EN.pdf, attached as **Exhibit 1**.

- "We give you control through your settings to limit the data we collect from you and how we use it, and to control things like account security, marketing preferences, apps that can access your account, and address book contacts you've uploaded to Twitter. You can also download information you have shared on Twitter." *Id.*, p. 2.

70. Most notably, § 3.1 of the Privacy Policy promises that:

> **We share or disclose your personal data with your consent or at your direction**, such as when you authorize a third-party web client or application to access your account or when you direct us to share your feedback with a business. . . .
>
> Subject to your settings, we also provide certain third parties with personal data to help us offer or operate our services. For example, we share with advertisers the identifiers of devices that saw their ads, to enable them to measure the effectiveness of our advertising business. We also share device identifiers, along with the interests or other characteristics of a device or the person using it, to help partners decide whether to serve an ad to that device or to enable them to conduct marketing, brand analysis, interest-based advertising, or similar activities. You can learn more about these partnerships in our Help Center, and **you can control whether Twitter shares your personal data in this way by using the "Share your data with Twitter's business partners" option in your Personalization and Data settings**. (This setting does not control sharing described elsewhere in our Privacy Policy, such as when we share data with our service providers.) **The information we share with these partners does not include your name, email address, phone number, or Twitter username,** but some of these partnerships allow the information we share to be linked to other personal information if the partner gets your consent first.

71. As described herein, Twitter did not abide by its Privacy Policy in that Plaintiff and Class Members did not "know what data" Twitter "collect[ed] from [them] and how [Twitter] use[d] it," nor did Plaintiff and Class Members "have meaningful control over both"; Twitter did not give its users "control through your settings to limit the data we collect from you and how we use it"; and most importantly Twitter did "share or disclose [users'] personal data" without their

"consent or at [their] direction; all contrary to the Privacy Policy.

72. Importantly, Cal. Bus. & Prof. Code § 22576 prohibits an "operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service" from "knowingly and willfully" or "negligently and materially" failing "to comply with" the "provisions of its posted privacy policy."

73. Here, Twitter either "knowingly and willfully" or "negligently and materially" failed "to comply with" the "provisions of its posted privacy policy," in violation of Cal. Bus. & Prof. Code § 22576.

74. The structure and other provisions of the Privacy Policy do not undermine this conclusion. For example, Privacy Policy § 1.1 states:

> You don't have to create an account to use some of our service features, such as searching and viewing public Twitter profiles or watching a broadcast on Periscope's website. **If you do choose to create an account, you must provide us with some personal data so that we can provide our services to you. On Twitter this includes a display name** (for example, "Twitter Moments"), a username (for example, @TwitterMoments), **a password, and an email address or phone number.** Your display name and username are always public, but you can use either your real name or a pseudonym. You can also create and manage multiple Twitter accounts, for example to express different parts of your identity.

75. Thereafter, § 1.3 states:

> **We use your contact information, such as your email address or phone number**, to authenticate your account and keep it - and our services - secure, and to help prevent spam, fraud, and abuse. We also use contact information to personalize our services, enable certain account features (for example, for login verification or Twitter via SMS), and to send you information about our services. If you provide us with your phone number, you agree to receive text messages from Twitter to that number as your country's laws allow. Twitter also uses your contact information to market to you as your country's laws allow, and to help others find your account if your settings permit, including through third-party services and client applications. You can use your settings for email and mobile notifications to control notifications you receive from Twitter. You can also unsubscribe from a notification by following the instructions contained within the notification or here.

76. Twitter has argued that the statement in § 1.3 that "Twitter also uses your contact information to market to you" permits its conduct here.

77. However, the term "contact information" is not expressly defined in the Privacy Policy, but rather reasonably refers only to the "personal data" referenced in § 1.1 that is required for account creation.

78. Nowhere does the Privacy Policy expressly speak to how the information at issue in this case—that provided for two-factor authentication, account recovery, and/or account re-authentication, as opposed to the "contact information" provided for account creation—may be used, much less permit its use for marketing purposes.

79. Accordingly, use of the information at issue here—that provided for two-factor authentication, account recovery, and/or account re-authentication—is governed by the broader language of § 3.1, which permits disclosure only "with your consent or at your direction," which Twitter neither sought nor obtained from Plaintiff and Class Members.[14]

V. Tolling of the Statute of Limitations

80. Any applicable statutes of limitations have been tolled under (1) the fraudulent concealment doctrine, based on Twitter's knowing and active concealment and denial of the facts alleged herein and (2) the delayed discovery doctrine, as Plaintiff did not and could not reasonably have discovered Twitter's conduct alleged herein until shortly before the Complaint was filed.

81. Twitter never disclosed, or adequately disclosed, that it would use the collected Personal Information of Plaintiff and Class Members for advertising purposes.

VI. Need for Equitable Relief

A. Twitter's Long History of Data Privacy Failures.

82. Twitter's violation of consumers' privacy rights is not new – it has been persistent and pervasive for at least a decade.

83. For example, even after the FTC's action in 2011, and in addition to the history of misdeeds described above, Twitter has had a number of data breach, data privacy, and account

[14] In the alternative, to the extent Plaintiff's claims fall outside sections 1.3 and 3.1, and thus are not subject to any contractual provision, a quasi-contract claim should properly lie.

hacking issues.[15]

84. In February 2013, Twitter announced a security incident that potentially impacted around 250,000 users. The company said that attackers were able to gain access to account information, specifically user names and email addresses.[16]

85. In May 2018, Twitter advised that every user's password—some 330 million—had been exposed in an internal system. The passwords were unencrypted in an internal log, making them readable to anyone who accessed that system.[17]

86. In December 2018, reports emerged describing a security flaw that exposed the phone number country codes of Twitter users, potentially allowing malicious actors to determine the countries accounts were based in, something with significant ramifications for political dissidents, protestors, whistleblowers, activists, and other users who may be targeted for retaliation or silencing.[18] The issue came through one of Twitter's support forms for contacting the company, and Twitter acknowledged that a large number of inquiries through the form came from IP addresses located in China and Saudi Arabia. Constine, *supra* note 18. While the issue was not publicly announced until December 2018, a security researcher informed Twitter about the problem two years prior by filing a bug report. However, that report was closed without action after Twitter deemed the issue did "not appear to present a significant security risk."[19]

87. In November 2019, two former Twitter employees were charged with spying for Saudi Arabia. They were accused of snooping into thousands of private accounts and gathering

---

[15] Michael X. Heiligenstein, FIREWALL TIMES, *Twitter Data Breaches: Full Timeline Through 2022*, Aug. 23, 2022, *available at* https://firewalltimes.com/twitter-data-breach-timeline/

[16] Heather Kelly, CNN, *Twitter hacked; 250,000 accounts affected*, Feb. 1, 2013, *available at* https://www.cnn.com/2013/02/01/tech/social-media/twitter-hacked/index.html ; *see also* Heiligenstein, *supra* note 15.

[17] Rachel Sandler, BUSINESS INSIDER, *Twitter is telling everyone to change their password after a bug left 330 million passwords exposed*, May 3, 2018, *available at* https://www.businessinsider.com/twitter-tells-all-330-million-users-to-change-their-password-after-bug-left-them-exposed-2018-5; *see also* Heiligenstein, *supra* note 15.

[18] Josh Constine, TECHCRUNCH, *Twitter bug leaks phone number country codes*, Dec. 17, 2018, *available at* https://techcrunch.com/2018/12/17/twitter-country-code-leak/ ; *see also* Heiligenstein, *supra* note 15.

[19] Zack Whittaker, TECHCRUNCH, *Twitter warned of phone country code leak two years ago — but did nothing, security researcher says*, Dec. 18, 2018, *available at* https://techcrunch.com/2018/12/18/twitter-warned-country-code-form-leak-bug-security-researcher/; *see also* Heiligenstein, *supra* note 15.

personal information on specific users at the behest of the foreign nation, focusing on accounts that were critical of the Saudi Arabian government. However, other account data was potentially exposed as the spies compiled some data in bulk. While Twitter stated that it limited access to sensitive information among its staff, these two employees succeeded in accessing private account details, despite lacking the official authorization to do so.[20]

88. In one of the most well-publicized and infamous issues, in July 2020, a hacker targeted the accounts of approximately 130 high-profile individuals, including Bill Gates, Barack Obama, and Kanye West, posting scam messages involving Bitcoin, claiming the account holder was "giving back" to their community by doubling all Bitcoin sent to their address and sending those funds back to the sender. The attackers accessed the accounts by using Twitter internal administration tools to bypass some security measures. The hackers were able to obtain over $100,000 in transfers as a result of this incident.[21]

89. In fact, Twitter's own former head of security, Peiter "Mudge" Zatko, went public with allegations that the company's cybersecurity and privacy practices were woefully insufficient. Mr. Zatko described "egregious deficiencies, negligence, willful ignorance, and threats to national security and democracy."[22] He further stated that after joining the company he "soon learned 'it was impossible to protect the production environment. All engineers had access. There was no logging of who went into the environment or what they did…. Nobody knew where data lived or whether it was critical, and all engineers had some form of critical access to the production environment.' Twitter also lacked the ability to hold workers accountable for information security lapses because it has little control or visibility into employees' individual work computers, Zatko claims, citing internal cybersecurity reports estimating that 4 in 10 devices do not meet basic

[20] Richard Gonzales, NPR.ORG, 2 Former Twitter Employees Charged With Spying For Saudi Arabia, Nov. 6, 2019, *available at* https://www.npr.org/2019/11/06/777098293/2-former-twitter-employees-charged-with-spying-for-saudi-arabia ; *see also* Heiligenstein, *supra* note 15.

[21] Joe Tidy & David Molloy, BBC, *Twitter hack: 130 accounts targeted in attack*, July 17, 2020, *available at* https://www.bbc.com/news/technology-53445090 ; *see also* Heiligenstein, *supra* note 15.

[22] Donie O'Sullivan, Clare Duffy & Brian Fung, CNN, *Ex-Twitter exec blows the whistle, alleging reckless and negligent cybersecurity policies*, Aug. 23, 2022, *available at* https://edition.cnn.com/2022/08/23/tech/twitter-whistleblower-peiter-zatko-security/index.html ; *see also* Heiligenstein, *supra* note 15.

security standards." O'Sullivan, Duffy & Fung, *supra* note 22.

90. Mr. Zatko stated "that **despite the company's claims to the contrary, it had 'never been in compliance' with what the FTC demanded more than 10 years ago**. As a result of its alleged failures to address vulnerabilities raised by the FTC as well as other deficiencies, he says, Twitter suffers an 'anomalously high rate of security incidents,' approximately one per week serious enough to require disclosure to government agencies. 'Based on my professional experience, peer companies do not have this magnitude or volume of incidents,' Zatko wrote in a February letter to Twitter's board after he was fired by Twitter in January." *Id*. (emphasis added).

91. This pattern and practice of lax data security and privacy practices exemplifies the company-culture that led to the claims at issue here.

B. Twitter Decimates Its Staff and Ability to Respect Users' Information.

92. On or about October 28, 2022, Twitter was acquired by Mr. Elon Musk.

93. In the immediate wake of the acquisition, Mr. Musk terminated CEO Parag Agrawal, CFO Ned Segal, and head of legal policy, trust, and safety Vijaya Gadde. "On November 10, Twitter's top privacy and security executives resigned, including Chief Information Security Officer Lea Kissner, the company's chief privacy officer, and chief compliance officer, according to several reports. On the same day, Twitter's head of trust and safety, Yoel Roth, who in recent days had publicly reassured people that Twitter was still following its content moderation policies, also left."[23]

94. "The week after he took over, Musk continued firing executives, including Twitter's ad chief, general manager of core tech, and chief marketing officer Leslie Berland . . . . Soon after, Musk started gutting Twitter's rank-and-file staff. He laid off an estimated 50 percent — upward of 3,700 employees — from the company." Ghaffary, *supra* note 23. "Around 4,400 out of 5,500 of Twitter's contractors were laid off, including heavy cuts to Twitter's content moderation teams." *Id*.

95. Mr. Musk also announced he planned to slash $1 billion from Twitter's

[23] Shirin Ghaffary, VOX, *A comprehensive guide to how Elon Musk is changing Twitter*, Nov. 24, 2022, *available at* https://www.vox.com/recode/23440075/elon-musk-twitter-layoffs-check-mark-verification

infrastructure costs, such as server space. *Id*.

96. "A week and a half after the first wave of layoffs, the drama intensified when Musk issued an ultimatum to employees: Work harder or quit. In a midnight email to staff, Musk wrote that, moving forward, Twitter will 'need to be extremely hardcore' and require employees to work 'long hours at high intensity.' The email linked to a form asking employees to confirm that they want to work at the 'new Twitter' by 5 pm ET the next day; if not, they would be laid off and receive three months severance . . . . So far, it's been reported that 1,200 employees declined to agree to Musk's terms and essentially mass resigned from the company." *Id*.

97. In fact, the Federal Trade Commission has expressed "'deep concern' about Twitter's compliance with security and privacy regulations after top executives resigned following the purchase of the social media company by billionaire Elon Musk, warning that enforcement actions may be on the horizon if past consent orders are violated. The abrupt resignation of Twitter's chief information security, privacy and compliance officers is raising concerns that Twitter is out of compliance with consent agreements it has entered with the FTC over the last two decades that require a designated senior-level team to be responsible for safeguarding user data. 'We are tracking recent developments at Twitter with deep concern,' Douglas Farrar, the FTC's director of public affairs, said in a statement. 'No CEO or company is above the law, and companies must follow our consent decrees. Our revised consent order gives us new tools to ensure compliance, and we are prepared to use them,' Farrar said."[24]

98. The mass layoffs and resignations has resulted, not surprisingly, in Twitter's inability to maintain its security and privacy commitments and gives Plaintiff and Class Members reasonable grounds for pursuing injunctive and equitable relief.

CLASS ACTION ALLEGATIONS

99. Plaintiff seeks relief on behalf of himself and as representatives of all others who are similarly situated. Pursuant to Code Civ. Proc. §382, and with guidance from Fed. R. Civ. P.

[24] Hannah Albarazi, LAW360, *Twitter In FTC Crosshairs As Top Privacy Execs Quit*, Nov. 10, 2022, *available at* https://www.law360.com/articles/1548674/twitter-in-ftc-crosshairs-as-top-privacy-execs-quit

Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a nationwide class defined as follows:

> All individuals residing in the United States who between May 2013 and September 2019 provided his or her telephone number(s) and/or email address(es) ("Personal Information") to Twitter for purposes of two-factor authentication, account recovery, and/or account re-authentication (the "Nationwide Class").

100. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

101. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

102. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

103. **Ascertainability**: Membership of the Class is defined based on objective criteria and individual Class Members will be identifiable from Twitter's records, including from Twitter's massive data storage, consumer accounts, and enterprise services. Based on information readily accessible to it, Twitter can identify Class Members who were victims of Twitter's impermissible collection and use of the Personal Information as alleged herein.

104. **Numerosity**: The Class consists of millions of individuals. Specifically, as noted above, according to the 2022 FTC Complaint, from May 2013, approximately two million users provided a telephone number to enable two-factor authentication; from June 2015, approximately 37 million users provided a telephone number or email address for account recovery purposes; and from September 2014, approximately 104 million users provided a telephone number or email address in response to a prompt for re-authentication. Accordingly, Class Members are so numerous that joinder of all members is impracticable. Class Members may be identified from

Defendant's records, including from Twitter's consumer accounts and enterprise services.

105. **Predominant Common Questions**: Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether, during the class period, Twitter disclosed, or adequately disclosed, the purposes for which it was collecting and using the Personal Information;

b. Whether, during the class period, Twitter used the collected Personal Information for purposes other than for two-factor authentication, account recovery, and/or account re-authentication, and, specifically whether Twitter used the Personal Information for marketing and/or advertising purposes;

c. Whether Twitter's practice of collecting and utilizing the Personal Information violated the 2011 Commission Order and/or the FTC Act;

d. Whether Twitter's practice of collecting and utilizing the Personal Information violated state and federal privacy laws;

e. Whether Twitter's practice of collecting and utilizing the Personal Information violated tort laws;

f. Whether Twitter has been unjustly enriched by its practice of collecting and utilizing the Personal Information;

g. Whether Plaintiff and Class Members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

h. Whether Plaintiff and Class Members have sustained damages as a result of Twitter's conduct and if so, what is the appropriate measure of damages or restitution.

106. **Typicality**: Plaintiff's claims are typical of the claims of other Class Members, as all Class Members were uniformly affected by Twitter's wrongful conduct in violation of law as complained of herein.

107. **Adequacy of Representation**: Plaintiff will fairly and adequately protect the interests of Class Members and have retained counsel that is competent and experienced in class

action litigation, including nationwide class actions and privacy violations. Plaintiff and his counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class Members. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of Class Members, and they have the resources to do so.

108. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of a single adjudication, economies of scale and comprehensive supervision by a single, able court. Furthermore, as the damages individual Class Members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for Class Members to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

109. **California Law Applies to the Entirety of the Class**: California's substantive laws apply to every Class Member, regardless of where in the United States the Class Member resides. Defendant's own Terms of Service explicitly states "The laws of the State of California, excluding its choice of law provisions, will govern these Terms and any dispute that arises between you and Twitter. All disputes related to these Terms or the Services will be brought solely in the federal or state courts located in San Francisco County, California, United States, and you consent to personal jurisdiction and waive any objection as to inconvenient forum." By choosing California law for the resolution of disputes covered by its Terms of Service, Twitter concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class Members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Class Members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by the Plaintiff and all Class Members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein

constitutionally permissible. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class and California has the greatest interest in applying its laws here.

110. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNT ONE: BREACH OF CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

111. Plaintiff hereby incorporates the previously-pleaded paragraphs as if fully stated herein.

112. Twitter's relationship with its users is governed by the Twitter Terms of Service, the Twitter Privacy Policy.

113. The Twitter Privacy Policy repeatedly promises Plaintiff and Class Members that Twitter respects their information and discloses such information only with users' consent.

114. Specifically, Twitter's 2018 Privacy Policy states:

- "We believe you should always know what data we collect from you and how we use it, and that you should have meaningful control over both. We want to empower you to make the best decisions about the information that you share with us." Privacy Policy, effective May 25, 2018, p. 1, *available at* https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-page-gdpr/pdfs/PP_Q22018_April_EN.pdf.
- "We give you control through your settings to limit the data we collect from you and how we use it, and to control things like account security, marketing preferences, apps that can access your account, and address book contacts you've uploaded to Twitter. You can also download information you have shared on Twitter." *Id.*, p. 2.

115. Most notably, § 3.1 of the Privacy Policy promises that:

> **We share or disclose your personal data with your consent or at your direction**, such as when you authorize a third-party web client or application to access your account or when you direct us to share your feedback with a business. . . .
>
> Subject to your settings, we also provide certain third parties with

> personal data to help us offer or operate our services. For example, we share with advertisers the identifiers of devices that saw their ads, to enable them to measure the effectiveness of our advertising business. We also share device identifiers, along with the interests or other characteristics of a device or the person using it, to help partners decide whether to serve an ad to that device or to enable them to conduct marketing, brand analysis, interest-based advertising, or similar activities. You can learn more about these partnerships in our Help Center, and **you can control whether Twitter shares your personal data in this way by using the "Share your data with Twitter's business partners" option in your Personalization and Data settings**. (This setting does not control sharing described elsewhere in our Privacy Policy, such as when we share data with our service providers, or through partnerships other than as described in our Help Center.) **The information we share with these partners does not include your name, email address, phone number, or Twitter username,** but some of these partnerships allow the information we share to be linked to other personal information if the partner gets your consent first.

116. Twitter breached these promises.

117. As described herein, Plaintiff and Class Members did not "know what data" Twitter "collect[ed] from [them] and how [Twitter] use[d] it," nor did Plaintiff and Class Members "have meaningful control over both"; Twitter did not give its users "control through your settings to limit the data we collect from you and how we use it"; and most importantly Twitter did "share or disclose [users'] personal data" without their "consent or at [their] direction"; all contrary to the Privacy Policy.

118. The structure and other provisions of the Privacy Policy do not undermine this conclusion. For example, Privacy Policy § 1.1 states:

> You don't have to create an account to use some of our service features, such as searching and viewing public Twitter profiles or watching a broadcast on Periscope's website. **If you do choose to create an account, you must provide us with some personal data so that we can provide our services to you. On Twitter this includes a display name** (for example, "Twitter Moments"), a username (for example, @TwitterMoments), **a password, and an email address or phone number.** Your display name and username are always public, but you can use either your real name or a pseudonym. You can also create and manage multiple Twitter accounts, for example to express different parts of your identity.

119. Thereafter, § 1.3 states:

> **We use your contact information, such as your email address or phone number**, to authenticate your account and keep it - and our services - secure, and to help prevent spam, fraud, and abuse. We also use contact information to personalize our services, enable certain account features (for example, for login verification or Twitter via SMS), and to send you information about our services. If you provide us with your phone number, you agree to receive text messages from Twitter to that number as your country's laws allow. Twitter also uses your contact information to market to you as your country's laws allow, and to help others find your account if your settings permit, including through third-party services and client applications. You can use your settings for email and mobile notifications to control notifications you receive from Twitter. You can also unsubscribe from a notification by following the instructions contained within the notification or here.

120. The statement in § 1.3 that "Twitter also uses your contact information to market to you" does not permit the conduct here.

121. The term "contact information" is not expressly defined in the 2018 Privacy Policy, but rather reasonably refers only to the "personal data" referenced in § 1.1 that is required for account creation.

122. Nowhere does the Privacy Policy expressly speak to how the information at issue in this case—that provided for two-factor authentication, account recovery, and/or account re-authentication, as opposed to the "contact information" provided for account creation—may be used, much less permit its use for marketing purposes.

123. Accordingly, use of the information at issue here—that provided for two-factor authentication, account recovery, and/or account re-authentication—is governed by the broader language of § 3.1, which permits disclosure only "with your consent or at your direction," which Twitter neither sought nor obtained from Plaintiff and Class Members.

124. Plaintiff and Class Members fulfilled their obligations under the relevant contracts and are not in breach of any material terms.

125. As a result of Twitter's breach(es), Twitter was able to obtain the personal property of Plaintiff and Class Members and earn unjust profits.

126. Plaintiff and Class Members also did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of the Personal Information they agreed to share, which has ascertainable value to be proven at trial.

127. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages, consequential damages, nominal damages, and/or non-restitutionary disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

COUNT TWO: BREACH OF IMPLIED CONTRACT
(Alleged In the Alternative to Count I)
(On Behalf of Plaintiff and the Nationwide Class)

128. Plaintiff hereby incorporates the previously-pleaded paragraphs as if fully stated herein.

129. Defendant solicited and collected the Personal Information of Plaintiff and Class Members with the express representation that it would be used for two-factor authentication, account recovery, and/or account re-authentication.

130. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to utilize the Personal Information solely for the purposes expressed: two-factor authentication, account recovery, and/or account re-authentication, and for no other purposes such as marketing and/or advertising.

131. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their Personal Information to Defendant.

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

133. Defendant breached the implied contracts it made with Plaintiff and the Class by utilizing and profiting from their Personal Information via the marketing and advertising purposes the information was put to.

134. As a result of Defendant's breach of implied contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT THREE: UNFAIR COMPETITION LAW ("UCL"), CAL. BUS. & PROF. CODE § 17200 *ET SEQ.*
(On Behalf of Plaintiff and the Nationwide Class)

135. Plaintiff hereby incorporates the previously-pleaded paragraphs as if fully stated herein.

136. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200 (UCL). By engaging in the practices aforementioned, Twitter has violated the UCL.

137. Twitter's "unlawful" acts and practices include its violation of the 2011 Commission Order and Section 5 of FTC Act, violation of the Privacy Shield and Frameworks, and violation of Cal. Bus. & Prof. Code § 22576.

138. Twitter's conduct violated the spirit and letter of these laws, which prohibit unauthorized disclosure and collection of personal information.

139. Twitter's "unfair" acts and practices include its misrepresentations regarding, and failure to disclose the purposes for which it was collecting and utilizing, the Personal Information, as described above, and its subsequent use of that information for profit.

140. Plaintiff and Class Members have suffered injury-in-fact, including the loss of money and/or property as a result of Twitter's unfair, unlawful, and/or fraudulent practices, to wit, the unauthorized disclosure and use of their Personal Information which has value as demonstrated by its use for targeted advertising by Twitter. Plaintiff and Class Members have suffered harm in the form of diminution of the value of their private and personally identifiable data and content.

141. Twitter's actions caused damage to and loss of Plaintiff's and Class Members' property right to control the dissemination and use of their Personal Information.

142. Twitter reaped unjust profits and revenues in violation of the UCL. This includes Twitter's profits and revenues from its targeted-advertising services. Plaintiff and the Class seek restitution and disgorgement of these unjust profits and revenues.

143. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution, declaratory relief, reasonable attorneys' fees and costs under California

Code of Civil Procedure § 1021.5, injunctive relief, and all other equitable relief the Court determines is warranted.

COUNT FOUR: UNJUST ENRICHMENT
(Alleged In the Alternative to Counts 1 & 2)
(On Behalf of Plaintiff and the Nationwide Class)

144. Plaintiff hereby incorporates the previously-pleaded paragraphs as if fully stated herein.

145. Plaintiff and Class Members conferred a benefit on Twitter. Specifically, they provided Twitter with their Personal Information. In exchange, Plaintiff and Class Members should have received from Twitter the services that were the subject of the transaction—two-factor authentication, account recovery, and/or account re-authentication services—and should have been entitled to have Twitter not disclose and use their Personal Information for targeted advertising and/or marketing purposes.

146. Twitter knew that Plaintiff and Class Members conferred a benefit on Twitter and has accepted or retained that benefit. Twitter profited from the Personal Information of Plaintiff and Class Members for business purposes, without disclosing to, or obtaining authorization from, Plaintiff and Class Members to so use the Personal Information.

147. Thus, Twitter acquired the Personal Information through inequitable means in that it failed to disclose all the purposes for which it would use the Personal Information, and misrepresented those uses.

148. Plaintiff and Class Members have no adequate remedy at law.

149. Under the circumstances, it would be unjust for Twitter to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on it.

150. Twitter should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received—specifically all revenue related to the targeted advertising and/or marketing that utilized the improperly obtained Personal Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

A. Certify this action is a class action pursuant to Code Civ. Proc. § 382, and with guidance from Rule 23 of the Federal Rules of Civil Procedure;

B. Appoint Plaintiff to represent the Class;

C. Appoint undersigned counsel to represent the Class;

D. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class Members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

E. Award nominal damages to Plaintiff and the Class Members against Defendant;

F. Provide for non-restitutionary disgorgement of all of Defendant's profits that were derived, in whole or in part, from Twitter's collection and subsequent use of Plaintiff's and the Class Members' Personal Information;

G. Order Defendant to disgorge revenues and profits wrongfully obtained;

H. Enter an order enjoining Defendant's unlawful conduct alleged herein;

I. Award Plaintiff and Class Members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

J. Grant Plaintiff and the Class Members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all issues so triable.

DATED: March 10, 2023

Respectfully submitted,

/s/ Sophia M. Rios

Sophia M. Rios (SBN 305801)
BERGER MONTAGUE PC
401 B street, Suite 2000
San Diego, CA 92101
Telephone: (619) 489-0300
srios@bm.net

E. Michelle Drake, MN # 0387366*
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5999
Facsimile: (612) 584-4470
emdrake@bm.net

John A. Yanchunis*
Jean Sutton Martin*
Patrick Barthle*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jyanchunis@ForThePeople.com
jeanmartin@ForThePeople.com
pbarthle@ForThePeople.com

Michael F. Ram (SBN 104805)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@ForThePeople.com

Kate M. Baxter-Kauf, MN # 0392037*
Karen Hanson Riebel, MN # 219770*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (917) 471-1894
Fax: (865) 522-0049
jnelson@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

**pro hac vice* forthcoming

Counsel for Plaintiff and the Proposed Class