

1 TIFFANY CHEUNG (CA SBN 211497)
TCheung@mofo.com
2 MORRISON & FOERSTER LLP
425 Market Street
3 San Francisco, California 94105-2482
Telephone: (415) 268-7000
4 Facsimile: (415) 268-7522

5 PURVI G. PATEL (CA SBN 270702)
PPatel@mofo.com
6 MORRISON & FOERSTER LLP
707 Wilshire Boulevard, Suite 6000
7 Los Angeles, California 90017-3543
Telephone: (213) 892-5200
8 Facsimile: (213) 892-5454

9 Attorneys for Defendants
BUMBLE INC. and
10 BUZZ HOLDINGS L.P.

11 **UNITED STATES DISTRICT COURT**
12 **SOUTHERN DISTRICT OF CALIFORNIA**
13 **SAN DIEGO DIVISION**

15 RYAN CHIEN, individually and on behalf
16 of all others similarly situated,

17 Plaintiff,

18 v.

19 BUMBLE INC. and BUZZ HOLDINGS
20 L.P.,

21 Defendants.

Case No. **'22CV20 GPC NLS**

**DEFENDANTS BUMBLE
INC. AND BUZZ HOLDINGS
L.P.'S NOTICE OF
REMOVAL**

[28 U.S.C. § 1446(d)]

[Superior Court of the State of
California, County of San Diego;
Case No. 37-2021-00049769-CU-
MC-CTL]

22
23 TO THE CLERK OF THE UNITED STATES DISTRICT COURT, SOUTHERN
24 DISTRICT OF CALIFORNIA:

25 PLEASE TAKE NOTICE that Defendants Bumble Inc. (“Bumble”) and
26 Buzz Holdings L.P. (“Buzz Holdings”) (collectively, “Defendants”) hereby remove
27 this action from the Superior Court of the State of California, County of San Diego,
28 to the United States District Court for the Southern District of California pursuant

1 to 28 U.S.C. §§ 1332, 1441, 1446, and 1453.

2 **Procedural History and Timeliness of Removal**

3 1. On November 24, 2021, Ryan Chien (“Plaintiff”), on behalf of himself
4 and a purported nationwide class of all similarly situated individuals, filed a civil
5 action in the Superior Court of the State of California, County of San Diego,
6 entitled *Ryan Chien v. Bumble Inc. et al.*, Case No. 37-2021-00049769-CU-MC-
7 CTL. (Ex. 1, Declaration of Tiffany Cheung in Support of Defendants’ Notice of
8 Removal (“Cheung Decl.”) ¶ 2, Ex. A (“Compl.”).)

9 2. On December 8, 2021, Defendants received a copy of the complaint in
10 this action. (Ex. 2, Declaration of Kate Urquiola in Support of Defendants’ Notice
11 of Removal (“Urquiola Declaration” or “Urquiola Decl.”) ¶ 3.) This notice is
12 therefore timely. *See* 28 U.S.C. § 1446(b)(1) (removal is timely if filed within 30
13 days of defendant’s receipt of the pleading).

14 **Basis for Removal Jurisdiction**

15 3. Generally. The action is removable pursuant to the Class Action
16 Fairness Act of 2005 (“CAFA”), 28 U.S.C. §§ 1332(d) and 1453(b), for at least the
17 following reasons.

18 4. Covered Class Action. Plaintiff purports to bring this action on behalf
19 of a purported nationwide class of “[a]ll U.S. residents who registered for and/or
20 used the Bumble app during the applicable limitations period (the “Class”),” and a
21 subclass of “[a]ll residents of California who registered for and/or used the Bumble
22 app during the applicable limitations period.” (Compl. ¶ 117.) Plaintiff alleges that
23 Defendants engaged in “unlawful and intentional collection and use of users’
24 personally identifiable information . . . without their consent” and that “all Class
25 members . . . had their PII exposed or accessed in the Data Breach.” (*Id.* ¶¶ 1, 122.)

26 5. This action meets the CAFA definition of a class action, which is “any
27 civil action filed under Rule 23 of the Federal Rules of Civil Procedure or similar
28 State statute or rule of judicial procedure authorizing an action to be brought by 1 or

1 more representative persons as a class action.” 28 U.S.C. §§ 1332(d)(1)(B),
2 1453(a), (b).

3 6. Diversity. The minimal diversity standard of the CAFA is met so long
4 as any defendant is a citizen of a state different from any member of the putative
5 class of plaintiffs. *Id.* § 1332(d)(2)(A).

6 a. Plaintiff alleges that he is a citizen of California. (Compl. ¶ 18.)
7 The putative nationwide class includes members from every state. (*See id.* ¶ 117.)

8 b. As of the date the complaint was filed in the San Diego Superior
9 Court, and as of the date of this removal, Defendant Buzz Holdings is a Delaware
10 limited partnership with its principal place of business in Texas. (Urquiola Decl.
11 ¶ 5; *see* Compl. ¶¶ 19-21.) The only natural person in Buzz Holding’s partnership
12 chain is an individual domiciled in Austin, Texas. The only corporation in Buzz
13 Holding’s partnership chain is Defendant Bumble Inc., which is incorporated under
14 the laws of Delaware and has a principal place of business in Austin, Texas, where
15 its headquarters are located. The remaining partners or members that comprise the
16 limited liability companies and limited partnerships in Buzz Holding’s corporate
17 organization structure are Delaware citizens. (Urquiola Decl. ¶ 5.)

18 c. Accordingly, this action satisfies the diversity requirements of
19 the CAFA. 28 U.S.C. § 1332(d)(2)(A) because Plaintiff alleges at least any one
20 member of the purported class of plaintiffs (citizens of all states) is a citizen of a
21 state different from any one defendant (citizens of Delaware and Texas).

22 7. Amount in Controversy – Alleged Compensatory Damages. This
23 Court has original jurisdiction over a class action “in which the matter in
24 controversy exceeds the sum or value of \$5,000,000, exclusive of interest and
25 costs.” *Id.* § 1332(d)(2). The claims of the individual class members are
26 aggregated to determine whether the matter in controversy requirement is met. *Id.*
27 § 1332(d)(6). Where, as here, a complaint does not specify the amount of damages
28 sought, “a defendant can establish the amount in controversy by an unchallenged,

1 plausible assertion of the amount in controversy in its notice of removal.” *Ibarra v.*
2 *Manheim Invs.*, 775 F.3d 1193, 1197-98 (9th Cir. 2015). No submission of
3 evidence accompanying the removal notice is required. *Dart Cherokee Basin*
4 *Operating Co. v. Owens*, 574 U.S. 81, 89 (2014). Defendant’s burden requires
5 “only a plausible allegation that the amount in controversy exceeds the
6 jurisdictional threshold.” *Dart*, 574 U.S. at 89.

7 8. Plaintiff asserts eight causes of action against Defendants:

8 (1) Negligence, (2) Restitution and Unjust Enrichment, (3) Invasion of Privacy,
9 (4) Intrusion Upon Seclusion, (5) Violation of the California Unfair Competition
10 Law (“UCL”); (6) Violation of the California False Advertising Law (“FAL”);
11 (7) Violation of the California Consumer Privacy Act (“CCPA”), and (8) Violation
12 of the California Comprehensive Data Access and Fraud Act (“CDAFA”). (Compl.
13 ¶¶ 127-199.) Plaintiff’s negligence claim arises in part from a purported “data
14 breach” in March 2020 that Plaintiff alleges allowed access to Plaintiff’s and the
15 putative class’s “data and content.” (Compl. ¶ 136.) Among other things, Plaintiff
16 seeks to recover the cost of “identity protection and credit monitoring services” for
17 himself and the putative class members. (*Id.*) He further alleges the purported
18 breach reached “every one of [the Bumble app’s] 100M users.” (*Id.* ¶ 81.)

19 9. Defendants dispute Plaintiff’s allegations and dispute that they are
20 liable to Plaintiff or to the putative class.¹ Without conceding any merit to
21 Plaintiff’s damages allegations or causes of action, a plain reading of the complaint
22 demonstrates that the amount in controversy exceeds \$5,000,000 for purposes of
23 removal.

24 10. Plaintiff’s request for credit monitoring on behalf of himself and the
25 purported class alone exceeds this threshold. According to publicly available

26 _____
27 ¹ Defendants specifically reserve all rights to challenge the complaint on all
28 available grounds, including that Plaintiff improperly named Bumble and Buzz
Holdings as defendants in this action.

1 published sources, credit monitoring is likely to cost an average of approximately
2 \$7.50 per month. (See Ex. 1, Cheung Decl. ¶¶ 4-6, Exs. C-E.) Thus, the cost of
3 credit monitoring for just nine months would amount to approximately \$67.50 per
4 individual. As demonstrated by the attached Urquiola declaration, over 75,000
5 unique Bumble app users were associated with registration in the United States at
6 the time of the purported “data breach.” (Urquiola Decl. ¶ 4.) Thus, just nine
7 months of credit monitoring alone would place the amount in controversy over
8 \$5,000,000—satisfying the jurisdictional threshold without even taking into
9 account Plaintiff’s other claims.

10 11. Amount in Controversy – Statutory Damages. Plaintiff also alleges
11 that Defendants violated Section 1798.150 of the CCPA by failing “to prevent
12 Plaintiff’s and California Subclass members’ nonencrypted and nonredacted PII
13 from unauthorized disclosure” under “their duty to implement and maintain
14 reasonable security procedures and practices appropriate to the nature of the
15 information.” (Compl. ¶ 193.) The CCPA awards a minimum of \$100 and a
16 maximum of \$750 in statutory damages per violation of Section 1798.150. Cal.
17 Civ. Code § 1798.150(a)(1)(A). Though Plaintiff asserts that he currently seeks
18 only injunctive relief under the CCPA due to the 30-day curing period required by
19 the statute, Plaintiff affirms that he will seek leave to amend his complaint in order
20 to assert statutory damages once the curing period has elapsed. (Id. ¶ 195.) If such
21 an amended complaint is permitted and filed, the amount in controversy would
22 increase substantially and easily exceed the \$5,000,000 threshold.

23 12. Amount in Controversy – Punitive Damages and Injunctive Relief.
24 Plaintiff’s remaining requests for relief substantially increase the amount in
25 controversy. For instance, Plaintiff requests punitive damages and injunctive relief.
26 (Id. ¶¶ 156-57.) While Defendants dispute that Plaintiff is entitled to any such
27 relief, the value of the requested relief should be included in determining the
28 amount in controversy. See, e.g., *Guglielmino v. McKee Foods Corp.*, 506 F.3d

1 696, 700 (9th Cir. 2007) (punitive damages included in calculating amount in
2 controversy); *Cohn v. Petsmart, Inc.*, 281 F.3d 837, 840 (9th Cir. 2002) (injunctive
3 relief included in calculating amount in controversy).

4 13. Amount in Controversy – Attorneys’ Fees. Plaintiff also seeks an
5 award of attorneys’ fees. (Compl. ¶¶ 195,199; *see also* “Prayer for Relief”
6 subsection (c).) While Defendants dispute that any attorneys’ fees are recoverable,
7 this request should also be included in determining the amount in controversy. *See*
8 *Fritsch v. Swift Transp. Co. of Arizona, LLC*, 899 F.3d 785, 793 (9th Cir. 2018)
9 (reversing remand and holding that “attorneys’ fees are at stake in the litigation, and
10 must be included in the amount in controversy”).

11 14. Accordingly, based on Plaintiff’s allegations and the number of
12 Bumble app unique users nationwide at the time of the purported “data breach,” the
13 \$5,000,000 amount in controversy requirement is satisfied here, exclusive of
14 interest and costs.

15 15. No CAFA Exclusions. This action does not fall within any exclusion
16 to removal jurisdiction recognized by 28 U.S.C. § 1332(d). Plaintiff brings this
17 action on behalf of a nationwide class of “U.S. residents who registered for and/or
18 used the Bumble app during the applicable limitations period” and he does not
19 allege that over one-third of the putative class comprises citizens of California.
20 (Compl. ¶ 117.) Nor can the complaint as pleaded support such a conclusion.
21 Therefore, the exclusions to removal jurisdiction do not apply. *See* 28 U.S.C.
22 § 1332(d).

23 **Notice to State Court**

24 16. A copy of this Notice of Removal was filed with the Clerk of the
25 Superior Court of the State of California, San Diego County. (*See* Ex. 1, Cheung
26 Decl. ¶ 3, Ex. B, attaching without exhibits the state court removal notice.)
27
28

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

Intradistrict Assignment

17. Assignment of this action to the United States District Court for the Southern District of California is appropriate because this action was originally filed in the Superior Court of the State of California, San Diego County.

Accordingly, Defendants respectfully submit that this action is removed properly pursuant to the Class Action Fairness Act. By filing this Notice of Removal, Defendants do not waive, either expressly or implicitly, their right to assert any defense which it could have asserted in the Superior Court of the State of California for the County of San Diego.

Dated: January 6, 2022

MORRISON & FOERSTER LLP

By: /s/ Tiffany Cheung
TIFFANY CHEUNG

*Attorneys for Defendants
Bumble Inc. and
Buzz Holdings L.P.*

EXHIBIT 1

1 TIFFANY CHEUNG (CA SBN 211497)
TCheung@mofocom
2 MORRISON & FOERSTER LLP
425 Market Street
3 San Francisco, California 94105-2482
Telephone: (415) 268-7000
4 Facsimile: (415) 268-7522

5 PURVI G. PATEL (CA SBN 270702)
PPatel@mofocom
6 MORRISON & FOERSTER LLP
707 Wilshire Boulevard, Suite 6000
7 Los Angeles, California 90017-3543
Telephone: (213) 892-5200
8 Facsimile: (213) 892-5454

9 Attorneys for Defendants
BUMBLE INC. and
10 BUZZ HOLDINGS L.P.

11 **UNITED STATES DISTRICT COURT**
12 **SOUTHERN DISTRICT OF CALIFORNIA**
13 **SAN DIEGO DIVISION**

15 RYAN CHIEN, individually and on behalf
16 of all others similarly situated,

17 Plaintiff,

18 v.

19 BUMBLE INC. and BUZZ HOLDINGS
20 L.P.,

21 Defendants.

Case No. **'22CV20 GPC NLS**

**DECLARATION OF
TIFFANY CHEUNG IN
SUPPORT OF DEFENDANTS
BUMBLE INC. AND BUZZ
HOLDINGS L.P.'S NOTICE
OF REMOVAL**

[Superior Court of the State of
California, County of San Diego;
Case No. 37-2021-00049769-CU-
MC-CTL]

1 I, Tiffany Cheung, hereby declare as follows:

2 1. I am a member of the Bar of the State of California and a partner in the
3 law firm of Morrison & Foerster LLP, counsel of record for Defendants Bumble
4 Inc. and Buzz Holdings L.P. in the above-captioned action. I have personal
5 knowledge of the matters set forth below and, if called upon to do so, I could and
6 would testify competently thereto.

7 2. Attached as **Exhibit A** is a true and correct copy of the civil action
8 filed by Plaintiff Ryan Chien, purportedly on behalf of himself and all similarly
9 situated individuals, in the Superior Court for the State of California, County of San
10 Diego entitled *Ryan Chien v. Bumble Inc. et al.*, Case No. 37-2021-00049769-CU-
11 MC-CTL.

12 3. Attached as **Exhibit B** is a true and correct copy of the Notice of
13 Filing of Notice Removal (without exhibits) that was filed in the San Diego
14 Superior Court.

15 4. Attached as **Exhibit C** is a true and correct copy of Equifax's prices
16 for credit monitoring and identity theft protection as of January 5, 2022, as shown
17 on its website, quoting a minimum price of \$4.95 per month.

18 5. Attached as **Exhibit D** is a true and correct copy of Experian's
19 published prices for credit monitoring and identity theft protection as shown on its
20 website as of January 5, 2022, which quotes a minimum price of \$9.99 per month.

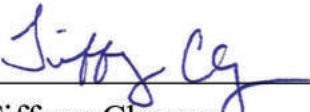
21 ///
22 ///
23 ///
24 ///
25 ///
26 ///
27 ///
28 ///

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

6. Attached as **Exhibit E** is a true and correct copy of Lifelock’s published prices for credit monitoring and identity theft protection as shown on its website as of January 5, 2022, which quotes a minimum price of \$7.50 per month.

I declare under penalty of perjury under the laws of the State of California and the United States that the foregoing is true and correct.

Executed this 6th day of January, 2022 in San Francisco, California.



Tiffany Cheung

TABLE OF EXHIBITS TO DECLARATION OF TIFFANY CHEUNG
(Pursuant to L.R. 5.1(e))

Exhibit	Description	Page(s)
A	Class Action Complaint, <i>Chien v. Bumble Inc. et al.</i> , San Diego Superior Court, Case No. 37-2021-00049769-CU-MC-CTL	4-48
B	Notice of Removal (without exhibits), <i>Chien v. Bumble Inc. et al.</i> , San Diego Superior Court, Case No. 37-2021-00049769-CU-MC-CTL	49-51
C	Equifax's prices for credit monitoring and identity theft protection as of December 16, 2021	52-54
D	Experian's published prices for credit monitoring and identity theft protection as shown on their website as of December 16, 2021	55-57
E	Lifelock's published prices for credit monitoring and identity theft protection as shown on their website as of December 16, 2021	58-61

EXHIBIT A

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
11/24/2021 at 12:08:34 PM
Clerk of the Superior Court
By Melissa Valdez, Deputy Clerk

Todd D. Carpenter
todd@lcllp.com
LYNCH CARPENTER, LLP
1350 Columbia Street, Suite 603
San Diego, CA 92101
Telephone: 619-762-1910
Facsimile: 412-231-0246

Attorneys for Plaintiff and the Proposed Classes

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF SAN DIEGO

RYAN CHIEN, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

BUMBLE INC., and BUZZ HOLDINGS L.P.,

Defendants.

Case No. 37-2021-00049769-CU-MC-CTL

**CLASS ACTION COMPLAINT FOR
DAMAGES AND INJUNCTIVE RELIEF
BASED ON:**

- 1. Negligence**
- 2. Restitution/ Unjust Enrichment**
- 3. Invasion of Privacy**
- 4. Intrusion Upon Seclusion**
- 5. Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 et seq.**
- 6. Violation of the California False Advertising Law, Cal. Bus. & Prof. Code §§ 17500 et seq.**
- 7. Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq.**
- 8. Violation of California Comprehensive Data Access and Fraud Act, Cal. Pen. Code § 502**

DEMAND FOR JURY TRIAL

Plaintiff Ryan Chien (“Plaintiff”) complains upon knowledge as to himself and his own actions and upon information and belief as to all other matters against Defendants Bumble Inc. and Buzz Holdings L.P. (collectively, “Bumble” or “Defendants”), as follows:

1 **I. SUMMARY OF ALLEGATIONS**

2 1. This action arises from Defendants’ unlawful and intentional collection and use
3 of users’ personally identifiable information, including biometric information (“PII”), without
4 their consent and subsequent unauthorized disclosure of that information in violation of state law.

5 2. In 2014, former Tinder founder Whitney Wolfe Herd partnered with Russian-
6 British billionaire technology entrepreneur Andrey Andreev to create Bumble, a dating app with
7 its mission to end misogyny by empowering women. Bumble is wildly popular and boasts
8 approximately one hundred million registered users worldwide.

9 3. Bumble is the dating app that puts the power in women’s hands. For a man to be
10 able to contact a woman, she must first have shown interest in him, adding a layer of privacy and
11 safety that other dating services lack.

12 4. Bumble shares a lot of the same features as the popular Tinder app, notably the
13 concept of “swiping right” to show your interest in a fellow user. Unlike Tinder, however,
14 women exclusively control the interactions in heterosexual communications on Bumble. Bumble
15 does this because the app is premised on safety and allowing users to control communications
16 and protect their privacy. Bumble touts the app as part of a movement create a more safe, kind,
17 and accountable internet.

18 5. Unbeknownst to its users, however, Defendants use automated software,
19 proprietary algorithms, AI, facial recognition, and other technologies to commercially profit
20 from Plaintiff’s and Class (defined below) members’ PII and identities, including unique
21 identifying information, biometric data and information, images, geolocation, names, e-mail
22 addresses, passcodes, social media accounts, messaging services, telephone numbers, and other
23 private, non-public, or confidential data and information, or meaningful combinations thereof,
24 as more fully set forth herein.

25 6. To use Bumble, users create and populate their profiles and Bumble collects
26 personal identifying information including: name; username; email address; mobile number;
27 gender identity; date of birth; sexual preference; photographs; location; and login information
28 for social media accounts connected to Bumble Account (including Facebook and Instagram

1 accounts). Users are required to create a password for their Bumble account during the
2 registration process.

3 7. Since Bumble is a dating app, users provide highly personal information in their
4 profile descriptions such as name, age, education, smoking and drinking preferences, voting
5 status, political preference, religious beliefs and zodiac sign. Users also upload photos to their
6 profiles.

7 8. Bumble also collects device information (unique device identifier, device model,
8 operating system, and MAC address) from its users along with other sensitive information. If
9 users purchase Bumble's premium services, Bumble processes and retains users' payment
10 information. Bumble also tracks user's interactions with links available on Bumble to third party
11 services and shares click statistics such as how many times a particular link was clicked.

12 9. Further, Bumble also collects data concerning its users' geolocation and
13 interactions with the site including data concerning sexual orientation and their "wish" (the types
14 of people they are looking to date based on their "swiping" record profile information).

15 10. Bumble harvests this extensive trove of data without the knowledge or consent of
16 its unsuspecting users and shares the collected data with third parties, including the social media
17 companies Facebook and Instagram.

18 11. Further, unbeknownst to its members, the app's photo verification feature scans
19 a user's facial geometry before running an algorithm to verify the user, collecting the user's
20 biometric information. Separately, the app's "Private Detector" feature, through artificial
21 intelligence, censors lewd content sent privately to users.

22 12. Users who registered for or used Bumble and interacted with the app did not
23 consent to Defendants' collection, retention, or release of their PII, including their biometric
24 information. Because of the app's emphasis on safety and security, Bumble customers trust that
25 their personal information will be maintained in a secure manner and kept from unauthorized
26 disclosure.

27 13. Defendants engaged in this conduct without adequately informing impacted
28 individuals, including Plaintiff and members of the proposed Classes, that their personal

1 information was being collected and disseminated. Worse, Bumble actively concealed the taking
2 of personal information through the use of “dark patterns” on the app, as described below.

3 14. What makes Defendants’ conduct even more egregious is that Bumble
4 experienced a data breach in March 2020 wherein an unauthorized individual was able to access
5 Bumble’s entire user database, exposing the profiles of all of its users. Bumble *never* disclosed
6 that the database had been breached and the user information exposed in this way.

7 15. This security breach left all of the profiles of Bumble users exposed for at least
8 8 months, and on information and believe, even longer. And despite Bumble’s public statements
9 that it addressed its security vulnerabilities, as of November 2020, Bumble user data was still
10 exposed.

11 16. To this day, Bumble has not even notified its users that their data was left
12 unprotected for such an extended period of time. Bumble’s negligent treatment of these security
13 vulnerabilities directly contradicts its assurances of security and privacy to its users.

14 17. Given the concealed and secretive nature of Defendants’ conduct, Plaintiff
15 believes that more evidence supporting the allegations in this Complaint will be uncovered after
16 a reasonable opportunity for discovery.

17 **II. PARTIES**

18 18. Plaintiff Ryan Chien is a natural person and citizen of the State of California and
19 a resident of San Diego County.

20 19. Defendant Bumble Inc., incorporated in Delaware on October 5, 2020, is an
21 American social media company that previously operated the Bumble online dating application.
22 Bumble Inc. maintained its principal place of business at 1105 West 41st Street, Austin, Texas
23 78756.

24 20. Prior to the completion of its initial public offering on February 16, 2021,
25 Bumble Inc. undertook certain reorganization transactions (the “Reorganization Transactions”)
26 such that Bumble Inc. is now a holding company, and its sole material asset is a controlling
27 equity interest in Defendant Buzz Holdings L.P. (“Bumble Holdings”). As the general partner of
28 Bumble Holdings, Bumble Inc. now operates and controls all of the business and affairs of

1 Bumble Holdings, has the obligation to absorb losses and receive benefits from Bumble Holdings
2 and, through Bumble Holdings and its subsidiaries, conduct its business.

3 21. Defendant Bumble Holdings is a Delaware limited partnership which operates the
4 Bumble app. Bumble Holdings maintains its principal place of business at 1105 West 41st Street,
5 Austin, Texas 78756.

6 **III. JURISDICTION AND VENUE**

7 22. This Court has subject-matter jurisdiction over this action pursuant to Cal. Code
8 Civ. Proc. § 410.10 and Article VI, § 10 of the California Constitution.

9 23. The Court has personal jurisdiction over Defendants because Defendants have
10 affirmatively established and maintained sufficient contacts with California and conduct
11 significant business in this State.

12 24. Defendants' deliberate gathering of California users' PII is intentionally targeted
13 toward California residents, including Plaintiff and the Classes, and constitutes purposeful
14 activity directed at devices and individuals in California.

15 25. Venue is proper in this County pursuant to Cal. Code Civ. Proc. § 395.5 as a
16 substantial portion of the transactions and allegations complained of herein occurred here.

17 **IV. FACTUAL ALLEGATIONS**

18 ***Background on the Bumble App***

19 26. Launched in 2014, Bumble is a popular dating app built for women, where women
20 make the first move. It is the second-most popular dating app in the U.S. after Tinder. As of
21 January 2021, the app has a monthly user base of 42 million people.

22 27. Users can sign up for Bumble using their phone number or Facebook profile.
23 Early on, Bumble users were required to log in via Facebook when signing up but in April 2018,
24 Bumble added an option to sign up with a phone number only.

25 28. For users who sign up with Facebook, information from their account is used to
26 build a profile with photos and personal information, including the user's college and job.

27
28

1 29. When in the app, users swipe right to “like” a potential match and left to reject
2 them. In heterosexual matches, only female users can make the first contact with matched male
3 users, while in same-sex matches either person can send a message first.

4 30. In addition to dating, Bumble offers users the opportunity to develop platonic
5 connections through Bumble BFF for friendships and Bumble Bizz for professional networking
6 and mentorship.

7 31. In March 2016, Bumble released BFF mode as a way for users to find platonic
8 friends. After switching into the mode, the app replaces potential dates with people of the user's
9 same sex who are also looking for friends.

10 32. In October 2017, the company launched Bumble Bizz which uses a woman-first
11 interface as an attempt to address sexism in business networking.

12 33. Bumble BFF and Bumble Bizz have a format similar to the dating app, requiring
13 users to set up profiles and matching users through “yes” and “no” votes, similar to the dating
14 platform.

15 34. Bumble represents the app platform to be safe and empowering for women to
16 provide a better dating environment for all users. In Defendants’ own words, “Bumble provides
17 opportunities to safely and easily connect with others.” See <https://bumble.com/en/date> (last
18 accessed 9/6/21).

19 35. In April 2016, the Bumble app was updated to combat “ghosting” behavior. As
20 part of the update, if a user is messaged after matching with a potential partner and fails to
21 respond within 24 hours, the match disappears. Before the update, men were allowed unlimited
22 time to respond to a message from women. This same update was also launched for same-sex
23 matches, with either party allowed to initiate and the other having to respond within 24 hours.

24 36. Protecting the identity of its users is at the very heart of the Bumble app. The
25 app’s central feature is that only women can initiate a conversation in heterosexual matches,
26 sparing users from the spamming that women often endure on other dating sites.

27
28

1 37. Bumble is marketed as an app which empowers women to make the first move
2 by giving them the ability to control the conversation thereby allowing users to create “safe and
3 healthy connections.”¹

4 38. According to Whitney Wolfe Herd, founder and CEO of Bumble, the app’s
5 growth in popularity is owed to the brand’s “safety, mission and women first narratives.”²

6 ***Bumble’s Data Collection Practices***

7 39. Bumble requires its customers to provide PII to use the app. It collects, retains,
8 and uses that data to maximize profits through predictive marketing and other targeted marketing
9 practices. By collecting, using, and deriving significant benefit from customers’ PII, Bumble had
10 a legal duty to take reasonable steps to protect this information from disclosure. As discussed
11 below, Defendants had a legal duty to take reasonable steps to protect customers’ PII under
12 applicable federal and state statutes, including Section 5 of the Federal Trade Commission Act,
13 15 U.S.C. § 45, and the California Consumer Protection Act of 2018 (the “CCPA”), Cal. Civ.
14 Code § 1798, *et seq.*

15 40. When a user downloads the app and creates an account, Bumble collects the
16 following information at registration: name; username; email address; mobile number; gender
17 identity; date of birth; sexual preference; photographs; location; and login information for social
18 media accounts connected to Bumble Account (including Facebook and Instagram accounts).
19 Users are required to create a password for their Bumble account during the registration process.

20 41. Bumble also collects device information (unique device identifier, device model,
21 operating system, and MAC address) from its users along with other sensitive information. If
22 users purchase Bumble’s premium services, Bumble processes and retains users’ payment
23 information. Bumble also tracks user’s interactions with links available on Bumble to third party
24 services and shares click statistics such as how many times a particular link was clicked.

25
26 ¹ See <https://bumble.com/en/help/what-is--bumble> (last accessed 9/6/21).

27 ² Levi Sumagaysay, Dating App Bumble Blows Past Expectations, Adding Users and Turning
28 a Profit, MarketWatch (May 12, 2021), available at <https://www.marketwatch.com/story/dating-app-bumble-blows-past-expectations-adding-users-and-turning-a-profit-11620852775>
(last accessed 9/6/21).

1 42. Many categories of information collected by Bumble from consumers fall within
2 recognized categories of “personal information” under the CCPA, including:

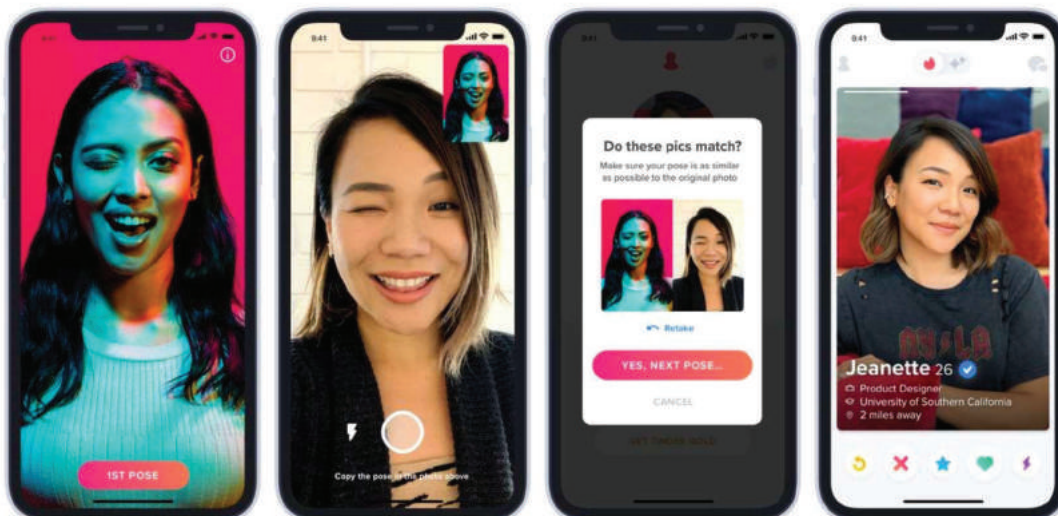
- 3 • Identifiers, such as name and location;
- 4 • Personal information, as defined in the California customer records law, such as
5 contact (including email and telephone number) and financial information;
- 6 • Characteristics of protected classifications under California or federal law, such
7 as age, gender identity, marital status, sexual orientation, race, ancestry, national
8 origin, religion, and medical conditions;
- 9 • Commercial information, such as transaction information and purchase history;
- 10 • Biometric information;³
- 11 • Internet or network activity information, such as browsing history and
12 interactions with our Bumble sites and the app;
- 13 • Geolocation data, such as mobile device location;
- 14 • Audio, electronic, visual and similar information, such as photos and videos;
- 15 • Professional or employment-related information, such as work history and prior
16 employer;
- 17 • Non-public education information; and
- 18 • Inferences drawn from any personal information to create a profile or summary
19 about, for example, an individual’s preferences and characteristics.⁴

20 43. Bumble launched a photo verification tool in September 2016 to ensure that users
21 were the same people in their profile pictures and with the stated goal of protecting users from
22 fake accounts. To be verified, users are asked to submit a selfie in a specific pose. The picture is
23 then reviewed through an automated process. Bumble employees may also conduct a review to
24 ensure the user is the person in the profile pictures.

25 _____
26 ³Though Bumble lists the collection of biometric information in its Privacy Policy, it states that
27 the category is “not relevant here.” As alleged herein, Bumble in fact collects biometric
28 information from its users which give rise to the violations asserted, and in contravention of its
own Privacy Policy.

⁴ See Bumble’s Privacy Policy, available at <https://bumble.com/privacy/> (last accessed 9/6/21).

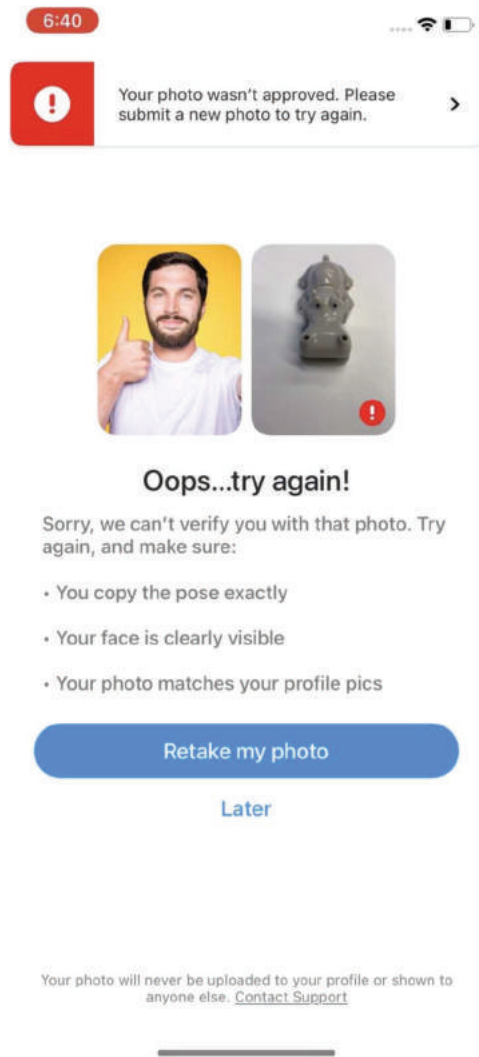
1 44. Bumble states that the verification feature is optional but encourages its use. To
2 verify an account, the user taps a “verify” button in their profile. They are then prompted with
3 an example of one of a hundred random photo poses created by Bumble and asked to take a selfie
4 mimicking that pose. After a user’s photo is reviewed, they quickly receive a confirmation or
5 rejection of their verification. Users are also encouraged to ask each other to validate their
6 profiles while chatting to make sure that they are talking to real people. Users who are reported
7 as potentially fake are rejected in verification have their profile turned off. If however a user’s
8 photo is verified, the user will continue using the app as normal. Photos used for photo
9 verification are not uploaded to the user’s profile.



10
11
12
13
14
15
16
17
18
19
20 45. In connection with its facial verification feature, Defendants implemented an
21 artificial intelligence tool that automatically performs facial scans. In doing so, the app extracts
22 geometric data relating to the unique points and contours (i.e., biometric identifiers) of each face,
23 and then uses that data to create a template of each face.

24 46. When people upload real selfies to the photo verification feature, the app may
25 take over a minute to analyze the photo and respond with an affirmation or rejection of the photo.
26 However, when faced with photos of a subject other than a human face, the photo verification
27 feature quickly responds with a rejection message. Thus, it is evident that the data is analyzed by
28 an automated system that scans the photo to recognize a face.

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



47. In 2017, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) released a document providing definitions for biometric information. According to this document, biometric recognition is defined as “automated recognition of individuals based on their biological and behavioural characteristics.”⁵

48. Moreover, the ISO/IEC document adds that “automated recognition implies that a machine based system is used for the recognition either for the full process or assisted by a human being.” *Id.*, at § 3.1.3, n.4. It is evident that Bumble automatically analyzes biometric information here.

⁵See https://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip (last accessed 9/6/21) at § 3.1.3.

1 ***Bumble’s Collection of Behavioral Data and Content Moderation***

2 49. Bumble “is the first major social platform to embrace behavioral guardrails and
3 content moderation as part of its business model.”⁶ Defendants leverage “innovative technology
4 solutions to create a more inclusive, safe and accountable way to connect online for all users
5 regardless of gender.”⁷

6 50. Bumble uses artificial-intelligence technology to conduct content moderation for
7 violations of its app standards like hate speech, even when no users report the behavior. The goal
8 is to identify people who are likely to engage in bad behavior before they do anything.

9 51. For example, according to Bumble’s Chief Product Officer, Bumble’s technology
10 scans profiles for violent images and recognizes at least 700 “stop words” inside of chats. Each
11 time the algorithm uncovers a violation, it is referred to a team of human moderators who then
12 decide whether blocking the user is appropriate. In 2020, Bumble “logged more than
13 880,000 incidents that violated its guidelines.”⁸ The company reported that its latest efforts are
14 tailored to address body shaming.⁹

15 52. Apart from content moderation, Bumble boasts that its proprietary machine
16 learning capabilities in selecting potential matches for users and determining which users are
17 likely to become paid members and to prevent identity fraud, among other things:

18 **Our data and machine learning capabilities:** We are continually analyzing data
19 from user interactions on our platform, allowing us to constantly optimize the
20 user experience. We have machine and deep learning capabilities that we leverage
21 to personalize the potential matches we display and to inform our product pipeline.
22 We are able to also target users who are likely to purchase a subscription package
23 or in-app feature and tailor the experience for them. Our machine and deep

24 ⁶ Charlotte Alter, How Whitney Wolfe Herd Turned a Vision of a Better Internet Into a Billion-
25 Dollar Brand, TIME (Mar. 19, 2021), available at <https://time.com/5947727/whitney-wolfe-herd-bumble/> (last accessed 9/6/21).

26 ⁷ See Bumble Inc. Form 10-K for the fiscal year ended 12/ 31/ 20 (the “2020 10-K”), available
27 at <https://ir.bumble.com/static-files/6873c49c-1778-4cbc-84ef-27b9d291bd53>, at p. 7 (last
28 accessed 9/6/21).

⁸ See Jane Wakefield, *The Tech Billionaire Who is Putting Women First*, BBC (Apr. 7, 2021),
<https://www.bbc.com/news/technology-56662100> (last accessed 9/6/21).

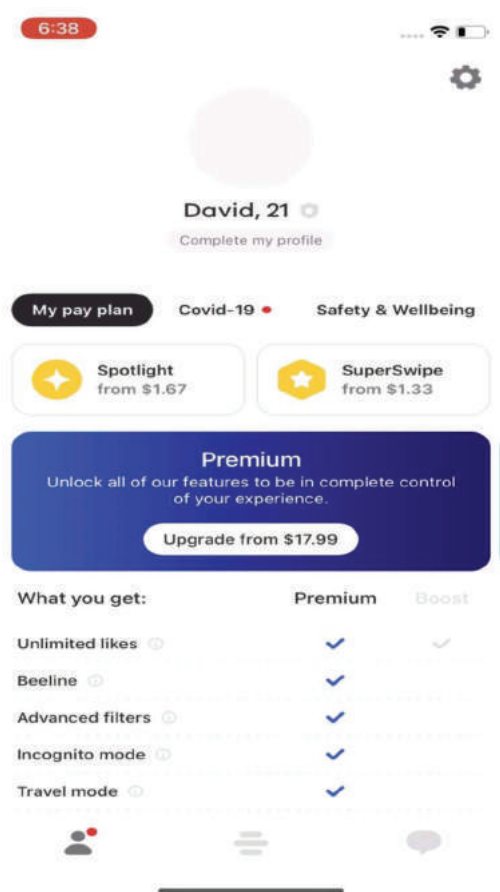
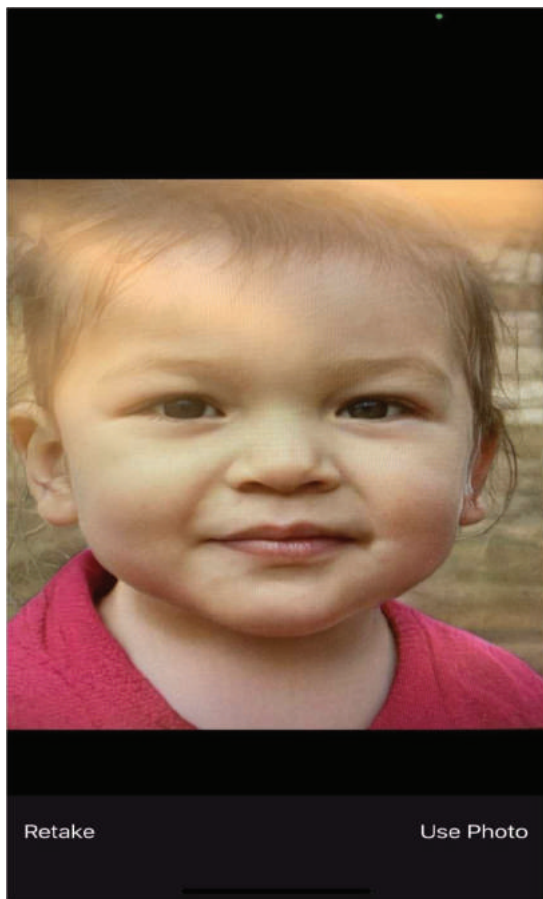
⁹ Charlotte Alter, How Whitney Wolfe Herd Turned a Vision of a Better Internet Into a Billion-
Dollar Brand, TIME (Mar. 19, 2021), <https://time.com/5947727/whitney-wolfe-herd-bumble/>
(last accessed 9/6/21).

1 learning posture plays a key role in identity fraud prevention as well as blocking
2 inappropriate behavior and content from polluting our platform.

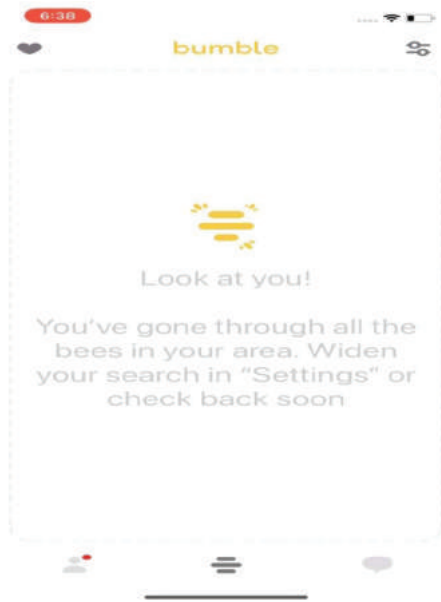
2020 10-K, at 8.

3 53. As such, Bumble also automatically analyzes its users' behavioral information
4 through its use of a matching algorithm which provides recommended potential connections to
5 the user based on the user's preferences and Bumble's research and analytics concerning and the
6 user's interactions with the app.

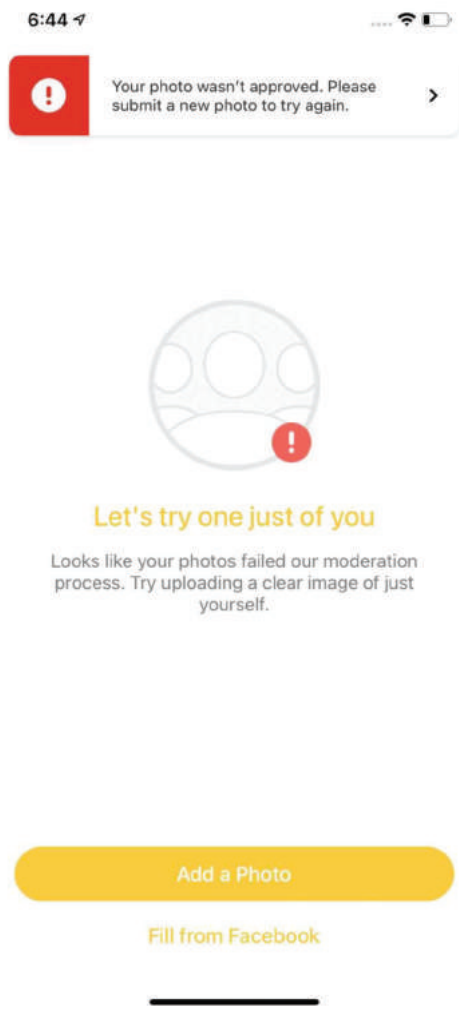
7 54. Once users have signed up for the app, they are required to add photos that meet
8 the app's guidelines. When users upload photos that do not include faces, the app immediately
9 blocks them and requires the user to upload others. The same is true when users upload photos
10 of children's faces. To clarify, when users upload pictures of objects or children, the app simply
11 fails to upload the pictures to the profile and tells the user that there are no relevant matches in
12 the area.



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



55. In some cases, users later receive notifications that their picture has been moderated:



1 56. Bumble’s machine learning technology also identifies and flags potentially
2 unwanted lewd images, which Bumble represents as a safety measure. The app’s “private
3 detector” artificial intelligence technology detects lewd pictures and blurs them out before
4 recipients see them.

5 57. Defendants unlawfully leverage user’s PII and private content to improve their
6 artificial intelligence technologies, thereby unjustly increasing their profits and revenues—and
7 Bumble’s market value.

8 58. Despite its use of facial recognition technology to moderate content and verify
9 users, Bumble denies that it captures or collects biometric information. While the app claims to
10 promote security and transparency, Defendants do not explicitly mention this collection to users.

11 59. The app’s privacy policy also fails to mention its retention policy regarding PII.
12 And, as detailed below, the app does not require users’ consent to its collection of biometric
13 information or to the app’s Privacy Policy in general. These practices contravene applicable
14 common law and California statutory law.

15 ***Bumble’s Use of Dark Patterns to Avoid Disclosing Data Collection Practices***

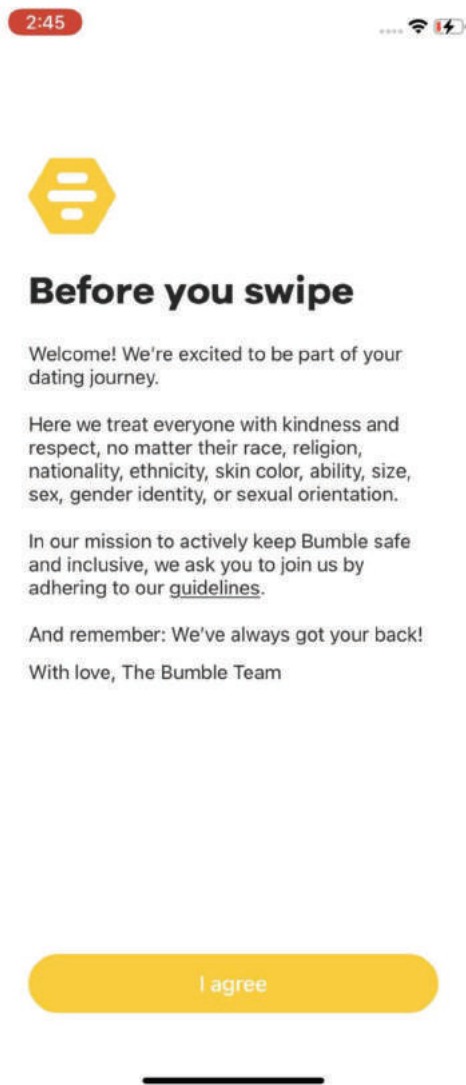
16 60. Though Bumble’s privacy policy appears to contain some disclosures concerning
17 its data collection practices, Bumble does not present these disclosures appropriately to
18 consumers. Plaintiff never received notice that Defendants would collect, capture, receive,
19 otherwise obtain, store, and/or use his PII. Plaintiff never signed a written release authorizing
20 Defendants to collect, capture, receive, otherwise obtain, store, and/or use his personal
21 information and biometric information.

22 61. In fact, based on counsel’s investigation and analysis, Defendants deliberately
23 designed Bumble’s Terms of Service and Privacy Policy to decrease the likelihood that a user
24 will notice and comprehend its terms and conditions or could provide meaningful, express
25 consent, in order to encourage users to sign up and not be deterred by accurate and truthful
26 disclosures.

27 62. Plaintiff did not know nor expect that Defendants would collect, store, and use
28 his PII when he used the app.

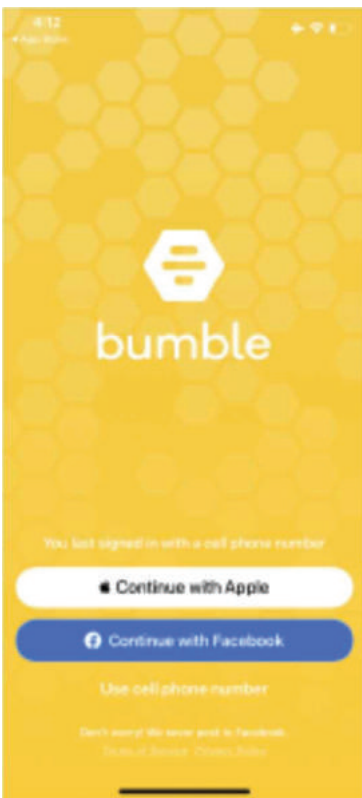
1 63. Defendants adopted Terms and Conditions for the app, not seen in the ordinary
2 course by users, which purport to disclose that the app takes some (but not all) of the private and
3 personally identifiable user data and content described above. Bumble’s Terms and Conditions,
4 revealed by investigation of counsel but not seen in the ordinary course by users, purport to
5 require arbitration and a class action waiver.

6 64. The app does not require that users sign and agree to its Terms and Conditions or
7 its Privacy Policy in order to use the app. It does, however, require that they agree to the app’s
8 Guidelines.



9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27 65. Thus, Bumble does not explicitly require app users to agree to the Terms and
28 Conditions or the app’s Privacy Policy. Moreover, links to the Terms and Conditions and Privacy

1 Policy are provided in extremely small letters on the bottom of the app’s sign-up page, presented
2 in almost the same hue as the app’s background:



16 66. Defendants’ design practice is termed a Dark Pattern, a user interface designed to
17 trick the user by purposely focus the person’s attention on one thing in order to distract their
18 attention from another. Bumble’s choice of elusive font and color guarantees that most new users
19 will not notice the presence of Bumble’s Terms and Conditions and Privacy Policy on their sign-
20 up page and will thus never read or agree to these terms.

21 67. Defendants never provided app users any actual notice of privacy policies or
22 terms of use. Nor do Defendants present users with conspicuously located and designed
23 hyperlinks to their privacy policies and terms of use, much less conspicuous warnings
24 accompanying such hyperlinks. The app thus allows users to utilize it without ever placing them
25 on actual or constructive notice of the privacy policies and terms of use. This lack of actual or
26 constructive notice deprives users of the opportunity to accept or reject Bumble’s privacy
27 policies and terms of use, rendering such documents unenforceable.

28

1 68. Even if Bumble users had knowingly accepted the terms of use (which they did
2 not), any purported waiver of the right to seek public injunctive relief in a court of law is
3 unenforceable under California law. *See, e.g., McGill v. Citibank*, 2 Cal. 5th 945 (2017); *Blair v.*
4 *Rent-A-Center*, 928 F.3d 819 (9th Cir. 2019).

5 69. The CCPA was recently amended to ban the use of Dark Patterns that prevent
6 users from opting out of the sale of their personal data.

7 70. Plaintiff and the Classes have incurred, and continue to incur, harm as a result of
8 the invasion of privacy stemming from Defendants’ covert theft of their private and personally
9 identifiable data and private content in the form of diminution of the value of their PII and content
10 as a result of Defendants’ surreptitious and unlawful activities.

11 71. Plaintiff and the Classes have also suffered and continue to suffer injuries to their
12 mobile devices. The battery, memory, CPU and bandwidth of such devices have been
13 compromised, and as a result the functioning of such devices has been impaired and slowed, due
14 to Defendants’ secretive and unlawful activities.

15 72. Defendants violated the CCPA in collecting and using personal information
16 without providing consumers with notice consistent with the CCPA, in violation of Civil Code
17 section 1798.100(b) and section 1798.115(d), and by otherwise failing to inform users of the
18 personal information collected about them and the third parties with whom that personal
19 information was shared, in violation of Civil Code section 1798.110(c).

20 73. Further, Defendants failed to use a reasonable standard of care to protect
21 Plaintiff’s and Class Members’ biometric identifiers and information from disclosure and, in fact,
22 affirmatively disclosed their biometric identifiers and information.

23 74. Particularly concerning are Defendants’ publicly announced plans to grow the
24 Bumble community so that Bumble’s “marketing learnings” can be shared “across our apps and
25 geographies, which enable the broadest application of successful strategies.”¹⁰

26
27
28

¹⁰ *See* 2020 10-K, at p. 10.

1 75. Per the app’s hidden Terms and Conditions, Bumble may assign or license users’
2 content to its “affiliates and successors without further approval” of its users.¹¹

3 ***The Data Breach***

4 76. In March 2020, a security researcher accessed Bumble’s entire user database of
5 nearly 100 million users and bypassed paying for the app’s premium services by finding and
6 exploiting the app’s security vulnerabilities (the “Data Breach”). The entire process required
7 only four days of work and application of a simple script.

8 77. Bumble’s vulnerabilities are derived from its Application Program Interface
9 (“API”) which essentially acts as a messenger that takes requests from Bumble users, transfers
10 them to the app’s system and returns the necessary response back to the user. When Bumble
11 users swipe on one another’s profiles, pay for premium features or access users’ photos, their
12 requests are processed using this technology.

13 78. Developers use APIs “to dictate how different parts of an application
14 communicate with each other and can be configured to allow client-side applications to access
15 data from internal servers and perform actions.” Developers program their API to check whether
16 the request issuer is authorized to perform a given action. Without these checks, hackers can
17 easily “manipulate API calls to perform unintended actions and retrieve unauthorized data.”

18 79. In Bumble’s case, the unauthorized researcher was able to reverse engineer its
19 web application’s API to intercept all of its incoming and outgoing requests. Bumble’s API did
20 not do the necessary checks and thus allowed the researcher to repeatedly probe the server for
21 information on Bumble users. According to the researcher, “these issues are relatively simple to
22 exploit, and sufficient testing would remove them from production. Likewise, fixing these issues
23 should be relatively easy as potential fixes involve server-side request verification and rate-
24 limiting.”¹²

25
26 ¹¹ See Bumble Terms and Conditions of Use (as of Apr. 28, 2021), available at
<https://bumble.com/en/terms> (last accessed 9/6/21).

27 ¹² See [https://www.forbes.com/sites/thomasbrewster/2020/11/15/bumble-vulnerabilities-put-](https://www.forbes.com/sites/thomasbrewster/2020/11/15/bumble-vulnerabilities-put-facebook-likes-locations-and-pictures-of-95-million-daters-at-risk/?sh=66492a2a3ddf)
28 [facebook-likes-locations-and-pictures-of-95-million-daters-at-risk/?sh=66492a2a3ddf](https://www.forbes.com/sites/thomasbrewster/2020/11/15/bumble-vulnerabilities-put-facebook-likes-locations-and-pictures-of-95-million-daters-at-risk/?sh=66492a2a3ddf) (last
accessed 9/6/21).

1 80. By exploiting the app’s vulnerabilities, the researcher was able to bypass
2 Bumble’s premium features, such as unlimited right swipes per day and the “Beeline” feature,
3 which lets users see the people who have swiped right on their profile, indicating interest in them.

4 81. More importantly, by intercepting the app’s API requests, the researcher was able
5 to enumerate Bumble’s worldwide users, reaching the individual identities of every one of its
6 100M users. The leaked data on each user included their public profile descriptions such as their
7 name, age, education, smoking and drinking preferences, voting status, political preference,
8 religious beliefs and zodiac sign.

9 82. More importantly, Bumble leaked users’ activity on the app, their sexual
10 orientation and their “wish”—the types of people they are looking to date based on their “swiping”
11 record. For each Bumble user, all of the pictures they had uploaded to the app were available to
12 the public and if they had connected the account to their Facebook account, the app leaked their
13 interests and pages they had liked.

```

14
15 {
16   "$gpb": "badoo.bma.Interest",
17   "interest_id": 1002530836,
18   "name": "Hugh Jackman",
19   "group_id": 12,
20   "category": 4,
21   "is_yours": false
22 },
23 {
24   "$gpb": "badoo.bma.Interest",
25   "interest_id": 1001177524,
26   "name": "In-N-Out Burger",
27   "group_id": 10,
28   "category": 2,
29   "is_yours": false
30 },
31 {
32   "$gpb": "badoo.bma.Interest",
33   "interest_id": 3632287,
34   "name": "Patrick Star",
35   "group_id": 12,
36   "category": 4,
37   "is_yours": false
38 },
39   "spoken_languages": [
40     {
41       "$gpb": "badoo.bma.Language",
42       "uid": 3,
43       "name": "English",
44       "level": 0
45     }
46   ],
47   "profile_fields": [
48     {
49       "$gpb": "badoo.bma.ProfileField",
50       "id": "education",
51       "type": 10,
52       "name": "Education",
53       "display_value": "<Redacted>"
54     },
55     {
56       "$gpb": "badoo.bma.ProfileField",
57       "id": "location",
58       "type": 1,
59       "name": "Location",
60       "display_value": "San Diego"
61     },
62     {
63       "$gpb": "badoo.bma.ProfileField",
64       "id": "wish",
65       "type": 1,
66       "name": "Wish",
67       "display_value": "Wants to date with girls, 18-23"
68     }
69   ]
70 }

```

26
27 83. Other troubling information that was leaked included whether they have the
28 mobile application installed, whether the app has rated them as “hot,” if they are online in real-

1 time, and their distance in miles from the person accessing the data. As hackers can easily fake
2 their location on the app, they could very easily track every user's exact location in real time.

3 84. The researcher disclosed the vulnerabilities and her findings to Bumble as soon
4 as March 30, 2020, but received no response from the company. She then made three more
5 attempts to contact the company in June and July 2020 and again, received no response. Two
6 hundred twenty-five days after the having been notified of the intrusion, Bumble had still not
7 responded to the researcher's request or taken any action to fix its security flaws. When the
8 researcher asked to publish the information, she received an email that "Bumble are keen to
9 avoid any details being disclosed to the press."

10 85. On November 1, 2020, the unauthorized researcher found that all of the attacks
11 still worked. When retesting on November 11, 2020, however, she found that certain issues had
12 been partially mitigated by Bumble. Specifically, at this point in time, the app's user database
13 could no longer be dumped and the app could not leak users' distance in miles. However, users'
14 Facebook interests, pictures and other profile information were still publicly available, even
15 when the researcher's Bumble user was locked-out and unvalidated.

16 86. To this day, Bumble has not notified its users of the vulnerabilities that left their
17 data unprotected for over 200 days. Moreover, Bumble's spokesperson denied the security flaw,
18 stating; "after being alerted to the issue we then began the multi-phase remediation process that
19 included putting controls in place to protect all user data while the fix was being implemented.
20 The underlying user security related issue has been resolved and there was no user data
21 compromised."

22 87. Nevertheless, the leaked data is extremely sensitive and detrimental to Bumble
23 users. A tech-savvy Bumble user could find the app's vulnerabilities and exploit them just as
24 easily as the security researcher above did. Such a user would have access to any profile that the
25 app would keep private in the normal course, with respect to users requesting that their profiles
26 be invisible to those who do not fit certain preferences of the profile-holder.

27 88. In some cases, the simple fact that a person is using the app could be problematic
28 if leaked. For example, if a Bumble user is married or in a relationship, the fact that she has an

1 active Bumble user profile, if revealed, may have detrimental effects on her personal life and can
2 thus be used to blackmail her. Moreover, LGBTQ users who have not publicly revealed their
3 sexual preferences but have indicated them on Bumble are extremely vulnerable to ransom
4 attacks and blackmail with heavy personal and professional consequences.

5 89. The fact that an unauthorized person was able to access Bumble’s user database
6 when her user was moderated and blocked is also extremely problematic. Bumble takes pride in
7 its secure features and claims to provide users with a safe and healthy space to meet others.
8 Bumble’s practices do not comport with the standards it promotes to its users.

9 90. It is also important to note that the app does not display users’ full names or links
10 to their Facebook accounts. This is done to maintain relative anonymity and protect users from
11 harassment. However, the leaked data provided access to users’ Facebook interests and likes and
12 thus to their profiles which include their full names and additional private details.

13 91. Bumble’s negligent treatment of these security vulnerabilities directly contradicts
14 its promises of security and privacy.

15 92. Plaintiff and Class members have suffered and will continue to suffer harm
16 because of the Data Breach. Malicious actors use PII to gain access to Class members’ digital
17 life, including bank accounts, social media, and credit card details. During that process, hackers
18 can harvest other sensitive data from the victim’s accounts, including personal information of
19 family, friends, and colleagues. The compromised PII is especially sensitive given the nature of
20 Defendants’ services.

21 93. The PII accessed in the Data Breach therefore has significant value to the hackers
22 who may attempt to sell that information. In fact, names, mailing and email addresses, dates of
23 birth, phone numbers, account information, and purchasing preferences are among the most
24 valuable pieces of information for hackers.

25 94. The PII accessed in the Data Breach is also very valuable to Defendants. Bumble
26 collects, retains, and uses this information to increase profits through predictive and other
27 targeted marketing. Bumble users value the privacy of this information and expect Bumble to
28 allocate enough resources to ensure it is adequately protected. Users would not have used

1 Bumble, uploaded personal photos, provided payment card information, and/or paid the same
2 prices for Bumble’s services had they known Bumble did not implement reasonable security
3 measures to protect their PII.

4 95. The PII accessed in the Data Breach is also very valuable to Plaintiff and Class
5 members. Consumers often exchange personal information for goods and services. For example,
6 consumers often exchange their personal information for access to wifi in places like airports
7 and coffee shops. Likewise, consumers often trade their names and email addresses for special
8 discounts (e.g., sign-up coupons exchanged for email addresses). Consumers use their unique
9 and valuable PII to access the financial sector, including when obtaining a mortgage, credit card,
10 or business loan. As a result of the Data Breach, Plaintiff and Class members’ PII has been
11 compromised and lost significant value.

12 96. Plaintiff and Class members will face a risk of injury due to the Data Breach for
13 years to come. Malicious actors often wait months or years to use the personal information
14 obtained in data breaches, as victims often become complacent and less diligent in monitoring
15 their accounts after a significant period has passed. These bad actors will also re-use stolen
16 personal information, meaning individuals can be the victim of several cyber crimes stemming
17 from a single data breach. Finally, there is often significant lag time between when a person
18 suffers harm due to theft of their PII and when they discover the harm. For example, victims
19 rarely know that certain accounts have been opened in their name until contacted by collections
20 agencies. Plaintiff and Class members will therefore need to continuously monitor their accounts
21 for years to ensure their PII obtained in the Data Breach is not used to harm them.

22 97. Plaintiff and Class members have and will continue to expend significant time
23 and money to reduce the risk of and protect against identity theft caused by the Data Breach.
24 According to the 2018 IBM/Ponemon Institute study, the average cost of a data breach in the
25 United States is \$242 per victim and roughly \$8 million per breach for companies. Where a
26 consumer becomes a victim of identity theft and suffers \$1 or more in direct or indirect losses,
27 the average cost to the consumer is \$1,343.

28

1 98. Even when reimbursed for money stolen due to a data breach, consumers are not
2 made whole because the reimbursement fails to compensate for the significant time and money
3 required to repair the impact of the fraud. On average, victims of identity theft spend 7 hours
4 fixing issues caused by the identity theft. In some instances, victims spend more than 1,000 hours
5 trying to fix these issues.

6 99. Victims of identity theft also experience harm beyond economic effects.
7 According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims
8 experienced negative effects at work (either with their boss or coworkers) and 8% experienced
9 negative effects at school (either with school officials or other students).

10 100. The U.S. Government Accountability Office likewise determined that “stolen
11 data may be held for up to a year or more before being used to commit identity theft,” and that
12 “once stolen data have been sold or posted on the Web, fraudulent use of that information may
13 continue for years.”¹³

14 ***Defendants Failed to Take Reasonable Steps to Protect Users’ PII***

15 101. Defendants require their users to provide a significant amount of highly personal
16 and confidential PII to use Bumble’s services. Defendants collect, stores, and uses this data to
17 maximize profits.

18 102. Defendants have legal duties to protect its customers’ PII by implementing
19 reasonable security features. This duty is further defined by federal and state guidelines and
20 industry norms.

21 103. Defendants breached their duties by failing to implement reasonable safeguards
22 to ensure Plaintiff’s and Class members’ PII was adequately protected. As a direct and proximate
23 result of this breach of duty, the Data Breach occurred, and Plaintiff and Class members were
24 harmed. Plaintiff and Class members did not consent to having their PII disclosed to any third-
25 party.

26
27
28 ¹³Available at <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm> (last accessed 9/6/21).

1 104. The Data Breach was a reasonably foreseeable consequence of Defendants’
2 inadequate security systems. Defendants have the resources to implement reasonable security
3 systems to prevent or limit damage from data breaches. Even so, Defendants failed to properly
4 invest in its data security. Had Defendants implemented reasonable data security systems and
5 procedures (i.e., followed guidelines from industry experts and state and federal governments),
6 then it likely could have prevented the infiltration of its systems and unauthorized access of its
7 users’ PII.

8 105. Defendants’ failure to implement reasonable security systems has caused Plaintiff
9 and Class members to suffer and continue to suffer harm that adversely impacts Plaintiff and
10 Class members economically, emotionally, and/or socially. As discussed above, Plaintiff and
11 Class members now face an imminent and ongoing threat of identity theft and resulting harm.
12 These individuals now must spend significant time and money to continuously monitor their
13 accounts and credit scores to limit potential adverse effects of the Data Breach regardless of
14 whether any Class member ultimately falls victim to identity theft.

15 106. Defendants also had a duty to timely discover the Data Breach and notify Plaintiff
16 and Class members that their PII had been compromised. Defendant breached this duty by failing
17 to use reasonable intrusion detection measures to identify the Data Breach when it occurred, and
18 then, once it learned of the Data Breach later, failing to inform affected users altogether.

19 107. Defendants failed to recognize the impact of the Data Breach on Bumble users;
20 they have not even offered impacted users credit monitoring services or other mitigation
21 measures beyond what is available to the public.

22 108. Even if Defendants had offered monitoring or other services to affected users, it
23 would be insufficient to protect Plaintiff and Class members. As discussed above, the threat of
24 identity theft and fraud from the Data Breach will extend for years and cost Plaintiff and the
25 Classes significant time and effort.

26 109. Plaintiff and Class members therefore have a significant and cognizable interest
27 in obtaining equitable relief (in addition to any monetary damages) that protects them from these
28 long-term threats. Accordingly, this action represents the enforcement of an important right

1 affecting the public interest and will confer a significant benefit on the general public or a large
2 class of persons.

3 ***Plaintiff's Experience***

4 110. Plaintiff is a Bumble user and has, within the applicable statute of limitations,
5 posted a profile on the app and uploaded and posted numerous images of his face to Bumble.

6 111. Defendants collected and stored Plaintiff's personal information and biometric
7 information. Upon information and belief, Defendants have disclosed and/or disseminated these
8 biometric identifiers or biometric information to third parties.

9 112. At no point did Plaintiff consent to or authorize Defendants to intercept, record,
10 disclose, or otherwise misuse his personal information or biometric information. Plaintiff would
11 not have registered for or used for Bumble had he known that Defendants engaged in the
12 unlawful actions described herein.

13 113. Plaintiff would like to continue to use Bumble in the future but will be uncertain
14 as to whether Defendants have ceased their unlawful practices and violation of his privacy rights
15 without the equitable relief requested herein, specifically an injunction prohibiting Defendants
16 from engaging in the unlawful practices alleged herein. This is particularly the case given the
17 surreptitious nature of Defendants' misconduct.

18 **V. FRAUDULENT CONCEALMENT AND TOLLING**

19 114. The applicable statutes of limitations are tolled as a result of Defendants' knowing
20 and active concealment of their unlawful conduct—through, among other things, their
21 obfuscation of the source code, misleading public statements, and hidden and ambiguous privacy
22 policies and terms of use. Plaintiff and the Classes were ignorant of the information essential to
23 pursue their claims, without any fault or lack of diligence on their own part.

24 115. Also, at the time the action was filed, Defendants were under a duty to disclose
25 the true character, quality, and nature of their activities to Plaintiff and the Classes. Defendants
26 are therefore estopped from relying on any statute of limitations.

27 116. Defendants' fraudulent concealment is common to the Classes.
28

1 **VI. CLASS ACTION ALLEGATIONS**

2 117. Plaintiff brings this action, individually, and on behalf of a class and subclass of
3 similarly situated persons, pursuant to Cal. Code Civ. Proc. § 382, Cal. Civ. Code § 1781, and
4 Cal. Bus. & Prof. Code § 17203, defined as follows:

5 **Nationwide Class**

6 All U.S. residents who registered for and/or used the Bumble app during the
7 applicable limitations period (the “Class”).

8 **California Subclass**

9 All residents of California who registered for and/or used the Bumble app during
the applicable limitations period. (the “California Subclass”)¹⁴

10 118. Excluded from the Class and California Subclass (collectively the “Classes”) are:
11 (1) any Judge or Magistrate presiding over this action and any members of their families;
12 (2) Defendants, Defendants’ subsidiaries, parents, successors, predecessors, and any entity in
13 which Defendants or their parents have a controlling interest and their current or former
14 employees, officers, and directors; (3) persons who properly execute and file a timely request for
15 exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated
16 on the merits or otherwise released; (5) Plaintiff’s counsel and Defendants’ counsel; and (6) the
17 legal representatives, successors, and assigns of any such excluded persons.

18 119. **Ascertainability.** The Classes are readily ascertainable because they are defined
19 using objective criteria so as to allow Class members to determine if they are part of the Classes.
20 Further, the Classes can be readily identified through records maintained by Defendants.

21 120. **Numerosity.** The Classes are so numerous that joinder of individual members
22 herein is impracticable. The exact number of Class members, as herein identified and described,
23 is not known, but publicly available information reveals that there are millions of app users in
24 the United States. California makes up roughly 12% of the nation’s population and is believed
25 to be home to a disproportionate number of Bumble users relative to other states.

26
27
28 ¹⁴ Plaintiff reserves the right to modify or refine the definition of the Classes.

1 121. **Commonality.** Common questions of fact and law exist for each cause of action
2 and predominate over questions affecting only individual Class members, including the
3 following:

4 a) whether Defendants engaged in the activities and practices referenced
5 above;

6 b) whether Defendants' activities and practices constitute a violation of the
7 California Comprehensive Data Access and Fraud Act, Cal. Pen. Code § 502;

8 c) whether Defendants' activities and practices constitute an intrusion upon
9 seclusion;

10 d) whether Defendants' activities and practices constitute a violation of the
11 California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et seq.*

12 e) whether Defendants' activities and practices constitute a violation of the
13 California False Advertising Law, Cal. Bus. & Prof. Code §§ 17500 *et seq.*;

14 f) whether Defendants violated § 1798.150 of the CCPA by failing to
15 prevent Plaintiff's and Class members' PII from unauthorized access and exfiltration,
16 theft, or disclosure as a result of Defendant's violations of its duty to implement and
17 maintain reasonable security procedures and practices appropriate to the nature of the
18 information;

19 g) whether Defendants owed Plaintiff and Class members a duty to
20 implement and maintain reasonable security procedures and practices to protect their
21 personal information;

22 h) whether Defendants' activities and practices constitute negligence;

23 i) whether Defendants adequately addressed and fixed vulnerabilities that
24 permitted the Data Beach to occur;

25 j) whether Defendants breached their duty to implement reasonable security
26 systems to protect Plaintiff's and the Class members' PII;

27 k) whether Defendants' breach of the duty to implement reasonable security
28 systems directly and/or proximately caused damages to Plaintiff and Class members;

1 l) whether and when Defendants learned of the Data Breach and whether the
2 response was adequate;

3 m) whether Plaintiff and other Class members are entitled to credit
4 monitoring and other injunctive relief;

5 n) whether Defendant provided timely notice of the Data Breach to Plaintiff
6 and Class members;

7 o) whether, prior to the Data Breach, Defendants knew or should have
8 known of the vulnerabilities in its systems that permitted them to be infiltrated;

9 p) whether Defendants' activities and data collection practices constitute
10 unjust enrichment concerning which restitution and/or disgorgement is warranted;

11 q) whether Plaintiff and members of the Class and Subclass sustained
12 damages as a result of Defendants' activities and practices, and, if so, in what amount;

13 r) whether Defendants profited from their activities and practices, and, if so,
14 in what amount;

15 s) what is the appropriate injunctive relief to ensure that Defendants no
16 longer unlawfully: **(i)** take private and personally identifiable user data and content;
17 **(ii)** utilize private and personally identifiable user data and content to develop
18 commercially valuable artificial intelligence technologies; **(iii)** utilize private and
19 personally identifiable user data and content to create consumer demand for and use of
20 Defendants' other products; **(iv)** cause the diminution in value of users' private and
21 personally identifiable data and content; **(v)** cause injury and harm to users' mobile
22 devices; **(vi)** cause users to incur higher data usage and electricity charges; **(vii)** retain
23 the unlawfully collected user data, including all personal information and biometric
24 information; and **(ix)** profile and target, based on the above activities, app users with
25 advertisements and other content.

26 t) what is the appropriate injunctive relief to ensure that Defendants take
27 reasonable measures to ensure that they and relevant third parties destroy unlawfully-
28 acquired user data and content in their possession, custody or control.

1 122. **Typicality.** Plaintiff’s claims are typical of the claims of members of the Classes
2 because, among other things, Plaintiff and members of the Classes sustained similar injuries as
3 a result of Defendants’ uniform wrongful conduct and their legal claims all arise from the same
4 events and wrongful conduct by Defendants. Further, all Class members were subject to the Data
5 Breach and had their PII exposed or accessed in the Data Breach. Likewise, Defendants’
6 misconduct impacted all Class members in the same manner.

7 123. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Classes.
8 Plaintiff’s interests do not conflict with the interests of the Class members, and Plaintiff has
9 retained counsel experienced in complex class action and data privacy litigation to prosecute this
10 case on behalf of the Classes.

11 124. **Predominance & Superiority.** Common questions of law and fact predominate
12 over any questions affecting only individual Class members, and a class action is superior to
13 individual litigation and all other available methods for the fair and efficient adjudication of this
14 controversy. The amount of damages available to Plaintiff is insufficient to make litigation
15 addressing Defendants’ conduct economically feasible in the absence of the class action
16 procedure. Individualized litigation also presents a potential for inconsistent or contradictory
17 judgments, and increases the delay and expense presented by the complex legal and factual issues
18 of the case to all parties and the court system. By contrast, the class action device presents far
19 fewer management difficulties and provides the benefits of a single adjudication, economy of
20 scale, and comprehensive supervision by a single court.

21 125. **Final Declaratory or Injunctive Relief.** Defendants have acted or refused to act
22 on grounds that apply generally to the Class and Subclass, making final declaratory and/or
23 injunctive relief appropriate with respect to the Class and California Subclass as a whole.

24 126. **Particular Issues.** The claims consist of particular issues that are common to all
25 Class and California Subclass members and are capable of class-wide resolution that will
26 significantly advance the litigation. These issues include but are not limited to:

- 27 a) whether Defendants unlawfully collected PII from consumers;

28

1 b) whether Defendants adequately disclosed their data collection practices to
2 consumers;

3 c) whether Defendants used dark pattens to gain access to consumers’ PII as
4 alleged herein;

5 d) whether Defendants owed a legal duty to Plaintiff and Class members to
6 exercise due care in collecting, storing, using and safeguarding their PII;

7 e) whether Defendants failed to comply with its own policies and applicable
8 laws, regulations and industry standards relating to data security;

9 f) whether Defendants failed to implement and maintain reasonable security
10 procedures and practices appropriate to the nature and scope of the information
11 compromised in the Data Breach; and

12 g) whether Plaintiff and Class members are entitled to actual damages, credit
13 monitoring, other injunctive relief, and/or punitive damages because of Defendants’
14 wrongful conduct.

15 **VII. CAUSES OF ACTION**

16 **FIRST CAUSE OF ACTION**
17 **Negligence**
18 **(On Behalf of the Plaintiff and the Class)**

19 127. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully
20 set forth herein.

21 128. Plaintiff and the Class entrusted Defendants with their PII and content never
22 intended for public consumption. Defendants had a duty to handle that data and content with care
23 due its sensitivity, and the expectation that such data and content would not be shared with third
24 parties or exposed in the Data Breach.

25 129. Plaintiff’s and the Class’s willingness to entrust Defendants with their PII and
26 private content was predicated on the understanding that Defendants would take appropriate
27 measures to protect this data. Defendants had a special relationship with the Plaintiff and the
28 Class as a result of being entrusted with their PII and content, which provided an independent
duty of care.

1 130. Defendants knew that the Plaintiff's and the Class's PII and content had value,
2 and Defendants have earned substantial revenues and profits as a result of collecting and using
3 PII and user content. This includes Defendants' profits and revenues from their targeted-
4 advertising, improvements to their artificial intelligence technologies, and the increased
5 consumer demand for and use of Defendants' other services.

6 131. Defendants failed to use reasonable care to safeguard the Plaintiff's and the
7 Class's PII and private content, giving third parties access to it without taking precautions to
8 protect the Plaintiffs and the Class.

9 132. Defendants' failure to use care in allowing access to the Plaintiff's and the Class's
10 private and personally identifiable data and private content resulted in the Data Breach and
11 caused foreseeable harm. Defendants failed to, inter alia: (i) implement security systems and
12 practices consistent with federal and state guidelines; (ii) implement security systems and
13 practices consistent with industry norms; (iii) timely detect the Data Breach; and (iv) timely
14 disclose the Data Breach to impacted customers.

15 133. Defendants knew or should have known Plaintiff's and Class members' PII was
16 highly sought after by hackers and that Plaintiff and Class members would suffer significant
17 harm if their PII was stolen.

18 134. Defendants also knew or should have known that timely disclosure of the Data
19 Breach was required and necessary to allow Plaintiff and Class members to take appropriate
20 actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing
21 accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges,
22 contacting financial institutions, and cancelling or monitoring government-issued IDs such as
23 passports and driver's licenses. The risk of significant harm to Plaintiff and Class members
24 (including identity theft) increases with the passage of time and continues to the present.

25 135. Defendants had a special relationship with Plaintiff and the Class members who
26 entrusted Defendants with several pieces of PII. Customers were required to provide PII when
27 utilizing Defendants' services. Defendants had a duty to protect that information. Plaintiff and
28 Class members were led to believe Defendants would take reasonable precautions to protect their

1 PII and would timely inform them if their PII was compromised, and Defendants breached their
2 duty when they failed to do so.

3 136. Defendants negligently allowed third parties to access Plaintiff's and the Class's
4 data and content, permitting it to be aggregated with other data and private content to identify,
5 profile and target Plaintiff and the Class. As such, it is reasonable for Plaintiff and the Class to
6 obtain identity protection and credit monitoring services, and to recover the cost of these services
7 from Defendants.

8 137. The injury to Plaintiff and the Class was a proximate, reasonably foreseeable
9 result of Defendants' breaches of duty. Defendants failed to enact reasonable security procedures
10 and practices and Plaintiff and Class members were the foreseeable victims of data theft that
11 exploited the inadequate security measures. The PII accessed in the Data Breach is precisely the
12 type of information that hackers seek and use to commit cyber crimes.

13 138. Defendants' conduct also constitutes gross negligence due to their extreme
14 departure from ordinary standards of care, and their knowledge that they had failed to secure the
15 Plaintiff's and the Class's PII and private content.

16 **SECOND CAUSE OF ACTION**
17 **Restitution / Unjust Enrichment**
18 **(On Behalf of the Plaintiff and the Class)**

19 139. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully
20 set forth herein.

21 140. Plaintiff and the Class have conferred substantial benefits on Defendants by
22 downloading and using the app. These include the Defendants' collection and use of the
23 Plaintiff's and the Class's PII and content never intended for public consumption. Such benefits
24 also include the revenues and profits resulting from Defendants' collection and use of such data
25 and content for Defendants' targeted-advertising, improvements to their artificial intelligence
26 technologies, and the increased consumer demand for and use of Defendants' other products.

27 141. Defendants knowingly and willingly accepted and enjoyed these benefits.

28 142. Defendants either knew or should have known that the benefits rendered by the
Plaintiff and the Class were given with the expectation that Defendants would not take and use

1 the Plaintiff's and the Class's PII and content that Defendants have taken and used without
2 permission. For Defendants to retain the aforementioned benefits under these circumstances is
3 inequitable.

4 143. Through deliberate violation of the Plaintiff's and the Class's privacy interests,
5 and statutory and constitutional rights, Defendants each reaped benefits that resulted in each
6 Defendant wrongfully receiving profits.

7 144. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants will
8 be unjustly enriched unless they are ordered to disgorge those profits for the benefit of the
9 Plaintiff and the Class.

10 145. As a direct and proximate result of Defendants' wrongful conduct and unjust
11 enrichment, the Plaintiff and the Class are entitled to restitution from Defendants and institution
12 of a constructive trust disgorging all profits, benefits, and other compensation obtained by
13 Defendants through this inequitable conduct.

14 **THIRD CAUSE OF ACTION**
15 **Invasion of Privacy**
16 **(On Behalf of Plaintiff and the Class)**

17 146. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully
18 set forth herein.

19 147. Plaintiff and the Class hold, and at all relevant times held, a legally protected
20 privacy interest in their PII and content on their mobile devices and in their other social media
21 accounts that Defendants have taken.

22 148. There is a reasonable expectation of privacy concerning Plaintiff's and the Class's
23 data and content under the circumstances present.

24 149. The reasonableness of Plaintiff's and the Class's expectation of privacy is
25 supported by the undisclosed, hidden, and non-intuitive nature of Defendants' taking of private
26 and personally identifiable data and content from Plaintiff's and the Class's mobile devices and
27 other social media accounts, through the use of dark patterns and otherwise.

28 150. Defendants' conduct constitutes and, at all relevant times, constituted a serious
invasion of privacy, as Defendants either did not disclose at all, or failed to make an effective

1 disclosure, that they would take and make use of – and allow third-party companies to take and
2 make use of—Plaintiff’s and the Class’s private and personally identifiable data and content.
3 Defendants intentionally invaded Plaintiff’s and the Class’s privacy interests by intentionally
4 designing the app to surreptitiously obtain, improperly gain knowledge of, review, and retain
5 their PII and content.

6 151. These intrusions are highly offensive to a reasonable person, as evidenced by
7 substantial research, literature, and governmental enforcement and investigative efforts to protect
8 consumer privacy against surreptitious technological intrusions.

9 152. The offensiveness of Defendants’ intrusion is heightened by Defendants’ making
10 Plaintiff’s and the Class’s private and personally identifiable data and content available to third
11 parties for a prolonged amount of time, without any notice. The offensiveness of Defendants’
12 intrusion is further heightened by Defendants’ clandestine collection and transfer of Plaintiff’s
13 and the Class’s private and personally identifiable data and content from their other social media
14 accounts. Further, Defendants’ conduct targeted Plaintiff’s and the Class’s mobile devices,
15 which the United States Supreme Court has characterized as almost a feature of human anatomy,
16 and which contain Plaintiff’s and the Class’s private and personally identifiable data and content.

17 153. Plaintiff and the Class were harmed by, and continue to suffer harm as a result of,
18 the intrusion as detailed throughout this Complaint.

19 154. Defendants’ conduct was a substantial factor in causing the harm suffered by
20 Plaintiff.

21 155. As a direct and proximate result of Defendants’ unlawful invasions of privacy,
22 Plaintiff’s and Class members’ reasonable expectations of privacy were frustrated and defeated.
23 Defendants’ unlawful invasions of privacy damaged Plaintiff and Class members as set forth
24 above, and they are entitled to appropriate relief.

25 156. Plaintiff and the Class seek nominal and punitive damages as a result of
26 Defendants’ actions. Punitive damages are warranted because Defendants’ malicious, oppressive,
27 and willful actions were calculated to injure Plaintiff and the Class, and were made in conscious
28

1 disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging
2 in future misconduct.

3 157. Plaintiff and the Class seek injunctive relief to rectify Defendants' actions,
4 including, but not limited to, requiring Defendants to stop taking more private and personally
5 identifiable data and content of Plaintiff and the Class from their mobile devices and their other
6 social media accounts than is reasonably necessary to operate the app; to make clear disclosures
7 of Plaintiff's and the Class's private and personally identifiable data and content that is
8 reasonably necessary to operate the app; to obtain Plaintiff's and the Class's consent to the
9 taking of their private and personally identifiable data and content; to stop transferring Plaintiff's
10 and the Class's private and personally identifiable data and content to third parties; and to recall
11 and destroy Plaintiff's and the Class's private and personally identifiable data and content
12 already taken in contravention of Plaintiff's and the Class's right to privacy under the common
13 law.

14 158. A person acting in conscious disregard of the rights of another is required to
15 disgorge all profit because disgorgement both benefits the injured parties and deters the
16 perpetrator from committing the same unlawful actions again. Disgorgement is available for
17 conduct that constitutes "conscious interference with a claimant's legally protected interests,"
18 including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd)
19 of Restitution and Unjust Enrichment, §§ 40, 44. Plaintiff and the Class seek restitution and
20 disgorgement for Defendants' violation of their privacy rights.

21 **FOURTH CAUSE OF ACTION**
22 **Intrusion Upon Seclusion**
(On Behalf of Plaintiff and the Class)

23 159. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully
24 set forth herein.

25 160. "One who intentionally intrudes, physically or otherwise, upon the solitude or
26 seclusion of another or his private affairs or concerns, is subject to liability to the other for
27 invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."
28 Restatement (2nd) of Torts § 652B.

1 161. Plaintiff and the Class have, and at all relevant times had, a reasonable expectation
2 of privacy in their mobile devices and their other social media accounts, and their private affairs
3 include their past, present and future activity on their mobile devices and their other social media
4 accounts.

5 162. The reasonableness of Plaintiff’s and the Class’s expectations of privacy is
6 supported by the undisclosed, hidden, and non-intuitive nature of Defendants’ taking of private
7 and personally identifiable data and content from Plaintiff’s and the Class’s mobile devices and
8 other social media accounts.

9 163. Defendants intentionally intruded upon the Plaintiff’s and the Class’s solitude,
10 seclusion, and private affairs—and continue to do so—by intentionally designing the app to
11 surreptitiously obtain, improperly gain knowledge of, review, and retain Plaintiff’s and the
12 Class’s PII and content.

13 164. These intrusions are highly offensive to a reasonable person, as evidenced by
14 substantial research, literature, and governmental enforcement and investigative efforts to protect
15 consumer privacy against surreptitious technological intrusions. The offensiveness of
16 Defendants’ intrusion is heightened by Defendants’ clandestine collection and transfer of the
17 Plaintiff’s and the Class’s PII and content from their other social media accounts. Further,
18 Defendants’ conduct targeted the Plaintiff’s and the Class’s mobile devices, which the United
19 States Supreme Court has characterized as almost a feature of human anatomy, and which
20 contain the Plaintiff’s and the Class’s private and personally identifiable data and content.

21 165. Plaintiff and the Class were harmed by, and continue to suffer harm as a result of,
22 the intrusion as detailed throughout this Complaint.

23 166. Defendants’ conduct was a substantial factor in causing the harm suffered by the
24 Plaintiff and the Class.

25 167. Plaintiff and the Class seek nominal and punitive damages as a result of
26 Defendants’ actions. Punitive damages are warranted because Defendants’ malicious, oppressive,
27 and willful actions were calculated to injure the Plaintiff and the Class and were made in
28

1 conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from
2 engaging in future misconduct.

3 168. Plaintiff and the Class seek injunctive relief to rectify Defendants' actions,
4 including, but not limited to, requiring Defendants to stop taking more private and personally
5 identifiable data and content from Plaintiff's and the Class's mobile devices and other social
6 media accounts than is reasonably necessary to operate the app; to make clear disclosures of
7 Plaintiff's and the Class's private and personally identifiable data and content that is reasonably
8 necessary to operate the app; to obtain Plaintiff's and the Class's consent to the taking of such
9 private and personally identifiable data and content; to stop transferring Plaintiff's and the
10 Class's private and personally identifiable data and content; and to recall and destroy Plaintiff's
11 and the Class's private and personally identifiable data and content already taken in
12 contravention of the Plaintiff's and the Class's privacy rights.

13 169. A person acting in conscious disregard of the rights of another is required to
14 disgorge all profit because disgorgement both benefits the injured parties and deters the
15 perpetrator from committing the same unlawful actions again. Disgorgement is available for
16 conduct that constitutes "conscious interference with a claimant's legally protected interests,"
17 including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd)
18 of Restitution and Unjust Enrichment, §§ 40, 44. Plaintiff and the Class seek restitution and
19 disgorgement for Defendants' intrusion upon seclusion.

20 **FIFTH CAUSE OF ACTION**
21 **Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 et seq.**
22 **(On Behalf of Plaintiff and the California Subclass)**

23 170. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully
24 set forth herein.

25 171. The Unfair Competition Law, California Business & Professions Code §§ 17200,
26 et seq. (the "UCL"), prohibits any "unlawful," "unfair," or "fraudulent" business act or practice,
27 which can include false or misleading advertising.

28 172. Defendants violated, and continue to violate, the "unlawful" prong of the UCL
through violation of statutes, constitutional provisions, and common law, as alleged herein.

1 173. Defendants violated, and continue to violate, the “unfair” prong of the UCL
2 because they took PII and content from Plaintiff’s and the California Subclass’s mobile devices
3 and other social media accounts under circumstances in which the Plaintiff and the California
4 Subclass would have no reason to know that such data and content was being taken.

5 174. Plaintiff and the California Subclass had no reason to know because there was no
6 effective disclosure of the wide range of PII and content that Defendants took from Plaintiff’s
7 and the California Subclass’s mobile devices and other social media accounts.

8 175. Defendants violated, and continue to violate, the “fraudulent” prong of the UCL
9 because Defendants made it appear that the Plaintiff’s and the California Subclass’s PII would
10 not be collected and transferred, but in fact, Defendants collected and transferred such data and
11 content without proper notice or consent; Defendants covertly transferred such data and content
12 to s third-party companies without notice or consent; and (Defendants intentionally refrained
13 from disclosing the use to which Plaintiff’s and the California Subclass’s private and personally
14 identifiable data and content has been put.

15 176. Plaintiff and the California Subclass were misled by Defendants’ concealment
16 and had no reason to believe that Defendants had taken the PII and private content that they had
17 taken.

18 177. In addition, Defendants engaged in unlawful acts and practices by maintaining
19 sub-standard security practices and procedures as described herein, by collecting and profiting
20 from Plaintiff’s and Class members’ PII knowing that it would not be adequately protected, and
21 by storing Plaintiff’s and Class members’ PII in an unsecure electronic environment in violation
22 of California’s data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to
23 implement and maintain reasonable security procedures and practices to safeguard the PII of
24 Plaintiff and the California Subclass.

25 178. In addition, Defendants engaged in unlawful acts and practices by failing to
26 disclose the Data Breach to the Plaintiff and the California Subclass in a timely and accurate
27 manner contrary to the duties imposed by Cal. Civ. Code §1798.82.
28

1 179. Plaintiff and the California Subclass have been harmed and suffered economic
2 injury as a result of Defendants’ UCL violations. First, Plaintiff and the California Subclass
3 suffered harm in the form of diminution of the value of their PII and content. Second, they
4 suffered harm to their mobile devices. The battery, memory, CPU and bandwidth of such devices
5 have been compromised, and as a result the functioning of such devices has been impaired and
6 slowed. Third, they incurred additional data usage and electricity costs that they would not
7 otherwise have incurred. Fourth, they suffered harm as a result of the invasion of privacy
8 stemming from Defendants’ covert theft of their PII and content. Fifth, they suffered harm
9 stemming from the exposure of their PII in the Data Breach.

10 180. Defendants, as a result of their conduct, have been able to reap unjust profits and
11 revenues in violation of the UCL. This includes Defendants’ profits and revenues from their
12 targeted-advertising, improvements to their artificial intelligence technologies and increased
13 consumer demand for and use of Defendants’ other products. Plaintiff and the California
14 Subclass seek restitution and disgorgement of these unjust profits and revenues.

15 181. Unless restrained and enjoined, Defendants will continue to misrepresent their
16 private and personally identifiable data and content collection and use practices and will not
17 recall and destroy Plaintiff’s and the California Subclass’s wrongfully collected private and
18 personally identifiable data and content. Accordingly, injunctive relief is appropriate.

19 **SIXTH CAUSE OF ACTION**
20 **Violation of the California False Advertising Law, Cal. Bus. & Prof. Code §§ 17500 *et seq.***
(On Behalf of Plaintiff and the California Subclass)

21 182. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully
22 set forth herein.

23 183. California’s False Advertising Law (the “FAL”), Cal. Bus. & Prof. Code
24 §§ 17500, *et seq.*, prohibits “any statement” that is “untrue or misleading” and made “with the
25 intent directly or indirectly to dispose of” property or services.

26 184. Defendants’ advertising is, and at all relevant times was, highly misleading.
27 Defendants do not disclose at all, or do not meaningfully disclose, the PII and content that they
28 have collected and transferred from the Plaintiff’s and the California Subclass’s mobile devices

1 and other social media accounts. Nor do Defendants disclose that the Plaintiff's and the
2 California Subclass's PII and content has been made available to third parties.

3 185. Reasonable consumers, like Plaintiff and the California Subclass, are—and at all
4 relevant times were—likely to be misled by Defendants' misrepresentations. Reasonable
5 consumers lack the means to verify Defendants' representations concerning their data and
6 content collection and use practices, or to understand the fact or significance of Defendants' data
7 and content collection and use practices.

8 186. Plaintiff and the California Subclass have been harmed and have suffered
9 economic injury as a result of Defendants' misrepresentations. First, they have suffered harm in
10 the form of diminution of the value of their private and personally identifiable data and content.
11 Second, they have suffered harm to their mobile devices. The battery, memory, CPU and
12 bandwidth of such devices have been compromised, and as a result the functioning of such
13 devices has been impaired and slowed. Third, they have incurred additional data usage and
14 electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as
15 a result of the invasion of privacy stemming from Defendants' covert theft of their PII and
16 content never intended for public consumption.

17 187. Defendants, as a result of their misrepresentations, have been able to reap unjust
18 profits and revenues from targeted-advertising, improvements to their artificial intelligence
19 technologies, and increased consumer demand for and use of Defendants' other products.
20 Plaintiff and the California Subclass seek restitution and disgorgement of these unjust profits and
21 revenues.

22 188. Unless restrained and enjoined, Defendants will continue to misrepresent their PII
23 data and content collection and use practices and will not recall and destroy Plaintiff's and the
24 California Subclass's wrongfully collected private and personally identifiable data and content.
25 Accordingly, injunctive relief is appropriate.
26
27
28

SEVENTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq.
(On Behalf of the Plaintiff and the California Subclass)

189. Plaintiff repeats and incorporates by reference all preceding paragraphs as if fully set forth herein.

190. The CCPA recently was enacted to protect consumers' personal information from collection and use by businesses without appropriate notice and consent.

191. Through the above-detailed conduct, Defendants violated the CCPA by, inter alia, collecting and using personal information without providing consumers with notice consistent with the CCPA, in violation of Civil Code section 1798.100(b) and section 1798.115(d), and by otherwise failing to inform users of the personal information collected about them and the third parties with whom that personal information was shared, in violation of Civil Code section 1798.110(c).

192. Defendants also violated the CCPA by failing to provide notice to their users of their right to opt-out of the disclosure of their biometric information to unauthorized third parties, like Facebook. Defendants did not give Plaintiff and the California Subclass members the opportunity to opt out before they provided their biometric information to unauthorized third parties. Indeed, regulations approved in March by California's Office of Administrative Law amended the existing CCPA regulations by expressly banning the use of dark patterns to subvert or impair the process for consumers to optout of the sale of personal information.¹⁵

193. Defendants also violated the CCPA by failing to prevent Plaintiff's and California Subclass members' nonencrypted and nonredacted PII from unauthorized disclosure as a result of Defendants' violation of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, in violation of Civil Code section 1798.150(a). Defendants' policies and practices failed to hold Plaintiff's and California Subclass members' personal information secure. This unauthorized dissemination and prolonged vulnerability of Plaintiff's and California Subclass members' personal information is exactly what the CCPA is intended to make actionable.

¹⁵ Cal. Code Regs. Tit. 11, Div. 1, Chap. 20 § 999.315(h).

1 194. In accordance with Civil Code section 1798.150(b), prior to the filing of this
2 complaint, Plaintiff’s counsel served Defendants with notice of these CCPA violations by
3 certified mail, return receipt requested.

4 195. On behalf of California Subclass members, Plaintiff seeks injunctive relief in the
5 form of an order enjoining Defendants from continuing to violate the CCPA. If Defendants fail
6 to respond to Plaintiff’s notice letter or agree to rectify the violations detailed above within
7 30 days of the date of written notice, Plaintiff also will seek leave to amend this Complaint to
8 assert claims for actual, punitive, and statutory damages, restitution, attorneys’ fees and costs,
9 and any other relief the Court deems proper as a result of Defendants’ CCPA violations.

10 **EIGHTH CAUSE OF ACTION**
11 **Violation of the California Comprehensive Data Access and Fraud Act**
12 **Cal. Pen. Code § 502**
(On Behalf of Plaintiff and the California Subclass)

13 196. Plaintiff repeats and incorporate by reference all preceding paragraphs as if fully
14 set forth herein.

15 197. Defendants’ acts violate Cal. Pen. C. § 502(c)(1) because they knowingly
16 accessed, and continue to knowingly access, data and computers to wrongfully control or obtain
17 data. Plaintiff’s and the California Subclass’s private and personally identifiable data and content
18 accessed by Defendants far exceeds any reasonable use of the Plaintiff’s and the California
19 Subclass’s data and content to operate the Bumble app. There is no justification for Defendants’
20 surreptitious collection and transfer of the Plaintiff’s and the Class’s PII and content from their
21 mobile devices and other social media accounts.

22 198. Defendants’ acts violate Cal. Pen. Code § 502(c)(2) because they have knowingly
23 accessed and without permission taken, copied, and made use of data from a computer—and
24 they continue to do so. Defendants did not obtain permission to take, copy, and make use of the
25 Plaintiff’s and the California Subclass’s private and personally identifiable data and content from
26 their mobile devices and their other social media accounts.

27 199. Plaintiff and the California Subclass are entitled to compensatory damages,
28 including “any expenditure reasonably and necessarily incurred by the owner or lessee to verify

1 that a computer system, computer network, computer program, or data was or was not altered,
2 damaged, or deleted by the access,” injunctive relief, and attorneys’ fees. Cal. Pen. Code
3 § 502(e)(1), (2).

4 **VIII. PRAYER FOR RELIEF**

5 WHEREFORE, Plaintiff respectfully requests for himself and all others similarly
6 situated, the following relief:

7 a. For an order certifying this action as a class action, defining the Class and
8 Subclass as requested herein, appointing the undersigned as Class counsel, and finding
9 Plaintiffs to be proper representatives of the Class and Subclass.

10 b. For a permanent injunction and any other equitable relief as necessary to protect
11 the interest of the Classes, including:

12 i. An order declaring Defendant’s conduct alleged herein unlawful and
13 prohibiting Defendant from engaging in the wrongful and unlawful acts; and

14 ii. Requiring Defendant to develop and adopt appropriate security protocols
15 to protect its consumers’ accounts, personal information, and privacy.

16 c. An award of all recoverable damages including punitive damages, as well as
17 attorneys’ fees and costs recoverable under the claims pleaded herein, as well as any such other
18 relief as is just and proper.

19 **IX. DEMAND FOR JURY TRIAL**

20 Plaintiffs demand a trial by jury on all issues so triable.

21 Dated: November 24, 2021

LYNCH CARPENTER, LLP

22 By: /s/ Todd D. Carpenter

Todd D. Carpenter (CA Bar No. 234464)

todd@lcllp.com

1350 Columbia St., Ste. 603

San Diego, California 92101

25 Tel: (619) 762-1900

26 Fax: (619) 756-6991

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

LYNCH CARPENTER, LLP
Katrina Carroll
katrina@lcllp.com
111 W. Washington St., Ste. 1240
Chicago, IL 60602
Tel.: 312-750-1265

*Attorneys for Plaintiff
and the Proposed Classes*

EXHIBIT B

1 TIFFANY CHEUNG (CA SBN 211497)
TCheung@mofo.com
2 MORRISON & FOERSTER LLP
425 Market Street
3 San Francisco, California 94105-2482
Telephone: (415) 268-7000
4 Facsimile: (415) 268-7522

5 PURVI G. PATEL (CA SBN 270702)
PPatel@mofo.com
6 MORRISON & FOERSTER LLP
707 Wilshire Boulevard, Suite 6000
7 Los Angeles, California 90017-3543
Telephone: (213) 892-5200
8 Facsimile: (213) 892-5454

9 Attorneys for Defendants
BUMBLE INC. and
10 BUZZ HOLDINGS L.P.

11 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
12 **COUNTY OF SAN DIEGO**

13 RYAN CHIEN, individually and on behalf of
14 all others similarly situated,

15 Plaintiff,

16 v.

17 BUMBLE INC. and BUZZ HOLDINGS L.P.,

18 Defendants.

Case No. 37-2021-00049769-CU-MC-CTL

**DEFENDANTS BUMBLE INC. AND BUZZ
HOLDINGS L.P.'S NOTICE OF FILING
OF NOTICE OF REMOVAL**

Hon. Eddie C. Sturgeon
Department: C-67
Trial Date: None Set
Date Action Filed: November 24, 2021

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

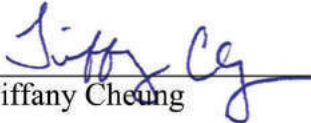
TO PLAINTIFF, HIS COUNSEL OF RECORD, AND THE CLERK OF THE SUPERIOR COURT OF THE STATE OF CALIFORNIA, COUNTY OF SAN DIEGO:

PLEASE TAKE NOTICE that on January 6, 2022, Defendants Bumble Inc. and Buzz Holdings L.P. filed a Notice of Removal of this action in the United States District Court for the Southern District of California. Attached to this Notice as **Exhibit 1** is a true and correct copy of the Notice of Removal (without exhibits).

PLEASE TAKE FURTHER NOTICE that, pursuant to 28 U.S.C. § 1446, the filing of this Notice affects the removal of this action to the federal court, and this Court is directed to “proceed no further unless and until the case is remanded.” 28 U.S.C. § 1446(d).

Dated: January 6, 2022

MORRISON & FOERSTER LLP

By: 
Tiffany Cheung

*Attorneys for Defendants
Bumble Inc. and
Buzz Holdings L.P.*

EXHIBIT C

My Personal Credit Compare our Value products


Compare our Value products

Discover which 1-Bureau credit score & report product makes the most sense for you.

Looking for 3-bureau credit features or additional identity protection tools? Compare our 3-bureau Premium products.

What You Need To Know:	EQUIFAX Core Credit™ Get the basics with your monthly credit score and report.	EQUIFAX Credit Monitor™ Easily lock ² and monitor your Equifax credit report with alerts.	EQUIFAX Complete™ Monitor your credit and help better protect your identity.
The credit score provided is a nonregulated 30 credit score based on Equifax data. Don't get too fixated on any one type of credit score and are likely to see a different type of credit score to make your creditworthiness.	FREE	\$4.95 / MONTH¹	\$9.95 / MONTH¹
Cancel at any time, no partial-month refunds.	GET STARTED	GET STARTED	GET STARTED
Features	Learn More	Learn More	Learn More
VantageScores and Equifax credit reports			
1-bureau credit score	Monthly	Daily	Daily
Equifax credit report ¹	Monthly	Daily	Daily
Credit monitoring			
Equifax credit report monitoring		✓	✓
Credit score monitoring		✓	✓
Identity theft			
Equifax credit report lock ²		✓	✓
Equifax blocked inquiry alerts		✓	✓
Automatic fraud alerts ⁴ <small>With a fraud alert, potential lenders are encouraged to take extra steps to verify your identity before extending credit.</small>			✓
Identity restoration			✓
Up to \$500k identity theft insurance ⁵			✓


Looking for 3-bureau credit features or additional identity protection tools? Check out these products:



Equifax Complete™ Premier

Take control with a one-stop credit monitoring² and identity theft protection solution from Equifax.

[LEARN MORE](#)



Equifax Complete™ Family Plan

Help look after your family with credit monitoring and ID theft protection features.

[LEARN MORE](#)

[COMPARE 3-BUREAU PRODUCTS](#)

- We will require you to provide your payment information when you sign up. We will immediately charge your card the price stated and will charge the card the price stated for each month you continue your subscription. You may cancel at any time; however, we do not provide partial-month refunds.
- Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit; or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.yourcreditreport.com.
- Under certain circumstances, access to your Equifax Credit Report may not be available as certain consumer credit files maintained by Equifax contain credit histories, multiple trade accounts, and/or an unreasonably number of inquiries of a nature that prevents or delays the delivery of your Equifax Credit Report, if a remedy for the failure is not available, the product subscription will be cancelled and a full refund will be made.
- The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.
- The Identity Theft Insurance benefit is underwritten and administered by American Banker's Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc. or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.
- Credit monitoring from Equifax and TransUnion will take several days to begin.

Account Settings | Personal Finance | Products & Tools

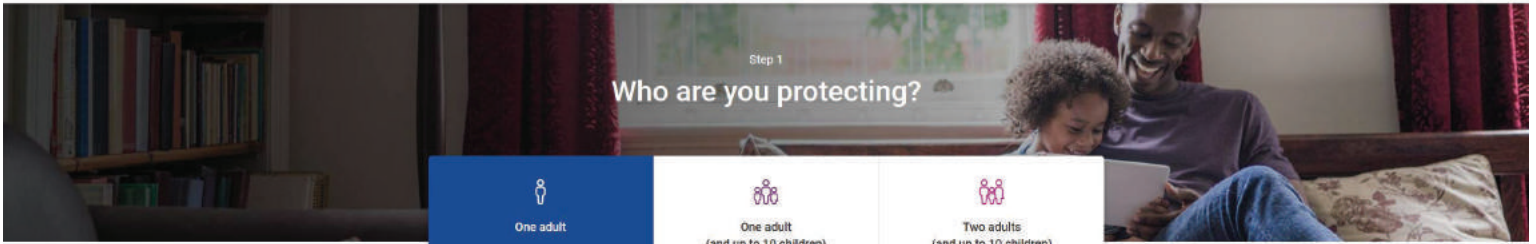
Compare Credit Monitoring Products | Loans | Life Stages | Cybersecurity | COVID - Credit | Knowledge Center

[Ad Choices](#) | [Accessibility](#) | [Do Not Sell My Personal Information](#) | [Privacy Policy](#) | [Terms of Use](#) | [Report a Vulnerability](#) | [Sitemap](#)


 Copyright 2022 Equifax, Inc. All rights reserved. Equifax and the Equifax marks used herein are trademarks of Equifax, Inc. Other product and company names mentioned herein are the property of their respective owners. Powering the World with Knowledge™

EXHIBIT D




Step 1


Who are you protecting?



One adult



**One adult
(and up to 10 children)**



**Two adults
(and up to 10 children)**

Step 2

Choose your plan level

IdentityWorks™ Plus

Free 30-day trial

then just \$9.99/month†

A full-featured plan that provides better identity theft detection, protection and resolution.

[Start for free](#)

[Compare benefits](#)

IdentityWorks™ Premium

Free 30-day trial

then just \$19.99/month†

Our best identity protection solution with 5-bureau credit monitoring and premium identity alerts.

[Start for free](#)

[Compare benefits](#)

IMPORTANT INFORMATION

A credit card is required to start your free 30-day trial membership† in Experian IdentityWorks™ Plus or Experian IdentityWorks™ Premium. You may cancel your trial membership at any time within 30 days without charge. If you decide not to cancel, your membership will continue and you will be billed \$9.99 each month for Experian IdentityWorks™ Plus or \$19.99 each month for Experian IdentityWorks™ Premium.

Billed Monthly Billed Annually (Save 17% annually)

IdentityWorks™ Plus

Free for 30 days, then just \$9.99/month†

[Start for free](#)

IdentityWorks™ Premium

Free for 30 days, then just \$19.99/month†

[Start for free](#)

Coverage

	One adult	One adult
Adult Identity Protection	✓	✓
Child Identity Protection	–	–
Social Security Number Trace	–	–
Social Network Monitoring	–	–
Dark Web Surveillance	–	–
Fraud Resolution Services	–	–
Identity Theft Insurance [®]	–	–

Identity Theft Monitoring & Protection

Dark Web Surveillance	✓	✓
Identity Theft Insurance [®]	Up to \$500,000	Up to \$1,000,000
U.S.-Based Fraud Resolution Specialist	✓	✓
Lost Wallet Assistance	✓	✓
Identity Theft Monitoring & Alerts	✓	✓
Social Security Number Monitoring	✓	✓
Address Change Verification	✓	✓
Financial Account Activity	–	✓
Identity Validation Alerts	–	✓
Payday Loan Monitoring	–	✓
Court Records	–	✓
Sex Offender Registry	–	✓
File-Sharing Network Monitoring	–	✓
Social Network Monitoring	–	✓

Experian CreditLock

Exhibit D

Real-time Alerts on Attempted Credit Inquiries	✓	✓
Credit Monitoring & Alerts		
Credit Bureaus Monitored	Experian	Experian, Equifax ¹ , TransUnion ²
New Credit Inquiries	✓	✓
New Accounts	✓	✓
Large Account Balance Changes	✓	✓
Credit Utilization	✓	✓
Positive Activity	✓	✓
Dormant Accounts	✓	✓
FICO [®] Score ³ Alerts	✓	✓
Credit Scores		
3-Bureau FICO [®] Scores ⁴	–	Quarterly
FICO [®] Scores ⁵ based on Experian data	Daily	Daily
Score Tracking	✓	✓
FICO [®] Score ⁶ Simulator	✓	✓
Additional FICO [®] Scores ⁷ (Auto, Home & Bankcard)	✓	✓

¹Monitoring with Experian begins within 48 hours of enrollment in your trial. Monitoring with Equifax[®] and TransUnion[®] takes approximately 4 days to begin, though in some cases cannot be initiated during your trial period. You may cancel your trial membership in IdentityWorksSM any time within 30 days of enrollment without charge.

²Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Review the Summary of Benefits for [Experian IdentityWorksSM Premium](#) or [Experian IdentityWorksSM Plus](#).

³Credit score is calculated based on FICO[®] Score 8 model, unless otherwise noted. In addition to the FICO[®] Score 8, we may offer and provide other base or industry-specific FICO[®] Scores (such as FICO[®] Auto Scores and FICO[®] Bankcard Scores). Your lender or insurer may use a different FICO[®] Score than FICO[®] Score 8 or such other base or industry-specific FICO[®] Score (if available), or another type of credit score altogether. [Learn more](#).

Credit & Identity Theft

- Free Credit Report
- Free Credit Score
- Free Credit Monitoring
- Free Experian Boost
- Experian CreditLock
- 3-Bureau Credit Report and FICO[®] Scores
- Identity Theft Protection
- What is a Good Credit Score
- Improving Your Credit Score
- How to Build Credit


CreditMatch

- Rewards Cards
- Cash Back Cards
- Low Interest Cards
- Balance Transfer Cards
- Secured Cards
- Cards for Bad Credit
- Cards for Fair Credit
- Personal Loans
- Credit Card Reviews
- Loan Reviews

Support

- Annual Credit Report
- Disputes
- Security Freeze
- Fraud Alert
- Identity Theft Victim Assistance
- Document Upload Service
- How to Dispute Report Information
- How to Place and Lift a Freeze


Get the Free Experian app:

Experian's Diversity, Equity and Inclusion

[Learn how we're committed](#)

Follow us

Legal Terms & Conditions
Privacy Policy
CA Privacy Policy
Press
Ad Choices
Careers
Investor Relations
Contact Us

© 2022 Experian. All rights reserved.
 Experian and the Experian trademarks used herein are trademarks or registered trademarks of Experian and its affiliates. The use of any other trade name, copyright, or trademark is for identification and reference purposes only and does not imply any association with the copyright or trademark holder of their product or brand. Other product and company names mentioned herein are the property of their respective owners. [Licenses and Disclosures](#).

EXHIBIT E

Identity theft protection all wrapped up.

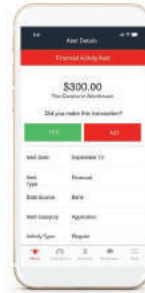
Identity thieves can take advantage of the season of giving. Now is the time to get the protection you need.

[SEE PLANS](#)

Speak to a live agent: 1-800-415-0599

How LifeLock works to help protect you against identity theft.

- 1 **SIGN UP**
It only takes a few minutes to enroll.
- 2 **WE SCAN**
We look for threats to your identity.
- 3 **WE ALERT!**
We alert you of potential threats by text, email or phone.^{††}
- 4 **WE RESOLVE**
If you become a victim of identity theft, a U.S.-based Identity Restoration Specialist will work to fix it.
- 5 **WE REIMBURSE**
We'll reimburse funds stolen due to identity theft up to the limit of your plan.^{†††}



Screenshots may be used for promotional purposes and subject to change.

††† Reimbursement and Expense Reimbursement, each with limits of up to \$1 million for Ultimate Plus, up to \$100,000 for Advantage and up to \$25,000 for Standard. And up to \$1 million for coverage for losses and repairs if needed, for all plans. Benefits under the Master Policy are issued and administered through Specialty Insurance Company (State of New York Insurance Company, Inc. or NY State Insurance), Special Policy Statement and/or at: Global Privacy Statement | Legal

Start your protection. Enroll in minutes.

- INDIVIDUAL**
1 Adult
- FAMILY PLAN**
2 Adults
- FAMILY PLAN**
2 Adults + 5 Kids

UP TO \$25,000 Reimbursement for Stolen Funds ^{†††}	UP TO \$100,000 Reimbursement for Stolen Funds ^{†††}	UP TO \$1 Million Reimbursement for Stolen Funds ^{†††}
LifeLock Standard	LifeLock Advantage	LifeLock Ultimate Plus
<input checked="" type="radio"/> Paid Annually \$7.50/month 1st yr \$80.00/yr <small>Pay up to \$25,000 reimbursement</small>	<input checked="" type="radio"/> Paid Annually \$14.99/month 1st yr \$179.88/yr <small>Pay up to \$100,000 reimbursement</small>	<input checked="" type="radio"/> Paid Annually \$19.99/month 1st yr \$239.88/yr <small>Pay up to \$1,000,000 reimbursement</small>
<input type="radio"/> Paid Monthly \$8.99/month 1st yr \$107.88/yr <small>Pay up to \$25,000 reimbursement</small>	<input type="radio"/> Paid Monthly \$17.99/month 1st yr \$215.88/yr <small>Pay up to \$100,000 reimbursement</small>	<input type="radio"/> Paid Monthly \$23.99/month 1st yr \$287.88/yr <small>Pay up to \$1,000,000 reimbursement</small>
START MEMBERSHIP	START MEMBERSHIP	START MEMBERSHIP
<small>What's new about?</small> \$25,000 Reimbursement for Stolen Funds ^{†††} ✓ Identity & Social Security Number Alerts [†] ✓ Credit Monitoring, One-Bureau [†]	<small>What's new about?</small> \$100,000 Reimbursement for Stolen Funds ^{†††} ✓ Identity & Social Security Number Alerts [†] ✓ Credit Monitoring, One-Bureau [†] ✓ Bank Account & Credit Card Activity Alerts [†] ✓ Alerts on Crimes in Your Name	<small>What's new about?</small> \$1 Million Reimbursement for Stolen Funds ^{†††} ✓ Identity & Social Security Number Alerts [†] ✓ Credit Monitoring, Three-Bureau [†] ✓ Bank Account & Credit Card Activity Alerts [†] ✓ Alerts on Crimes in Your Name ✓ Annual 3-Bureau Credit Reports + Credit Scores [†] ✓ 431(k) & Investment Account Activity Alerts [†]
Identity theft protection benefits (adult) ▾	Identity theft protection benefits (adult) ▾	Identity theft protection benefits (adult) ▾

Want Norton AntiVirus & VPN with LifeLock? [Click here](#)

Exhibit E

The credit scores provided are VantageScore 3.0 credit scores based on data from Equifax, Experian and TransUnion respectively. Any one bureau VantageScore mentioned is based on Equifax data only. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² If your LifeLock plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax, and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. **IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU.** If your plan also includes Credit Features from Equifax and/or TransUnion, the same verification process must also be successfully completed with Equifax and/or TransUnion as applicable. If verification is successfully completed with Equifax, but not with Equifax and/or TransUnion, or successfully you will not receive Credit Features from both bureaus. (iii) The verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Equifax and TransUnion will take several days to begin after your successful LifeLock plan enrollment.

[Click here for additional important information.](#)

Our Million Dollar Protection™ Package^{†††}



Personal Expense Compensation

We will cover you for personal expenses incurred as a result of identity theft, up to the limits of your plan.



Reimbursement of Stolen Funds

If your money is stolen due to ID theft, we will reimburse up to the amount provided by your plan.



Coverage for Lawyers and Experts

If you become a victim of identity theft while a LifeLock member, we will provide the necessary lawyers and experts if needed to help resolve your case.

^{†††} Reimbursement and Expense Compensation, each with limits of up to \$1 million for Ultimate Plus, up to \$100,000 for Advantage and up to \$25,000 for Junior and Smart, when purchased in Norton 360 with LifeLock Plus, and up to \$1 million for coverage for lawyers and experts provided, for all plans. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at [norton.lifelock.com/legal](#).

Trusted by millions for a reason.



MEMBER REVIEWS

Based on 9,000+ reviews of our identity theft protection on LifeLock.com



Join millions of Norton LifeLock members.

4.6/5



Based on 9,000+ reviews of our identity theft protection on LifeLock.com

<p>"GREAT SERVICE!" ★★★★★</p> <p><i>"I have had LifeLock for several years with upgrading to Ultimate Plus within the past year. They have thwarted attempts at my personal information twice in the past month. I would probably have never known of these if I hadn't had LifeLock. Thanks for taking care of this, LifeLock."</i></p> <p>Tina S. Current Ultimate Plus Member Member since Jan 2009</p>	<p>"THANK YOU!" ★★★★★</p> <p><i>"I was notified of fraudulent attempt to open a cell phone service in my name without my knowledge. I was asked to verify if it was me. When I said no the account was stopped. It made me feel thankful that someone was looking out for me."</i></p> <p>Joyce S. Current Member Member since Nov 2011</p>	<p>"BEST DECISION I'VE MADE!" ★★★★★</p> <p><i>"I started using LifeLock right after I tried to file my taxes and was told that my SSN had already been submitted. My tax guy suggested I try LifeLock. Best decision I made!"</i></p> <p>Jessie K. Current Advantage Member Member since Sept 2012</p>
--	---	--

WHAT ARE YOU WAITING FOR?

There was a victim of identity theft every 3 seconds in 2019.⁹

[START MEMBERSHIP](#)

It only takes minutes to sign up.

Identity theft protection is critical to your peace of mind

These days, identity theft protection strategies and tools are important ways to help protect your Social Security number and other personal information. A stolen identity can cost you money and time as you may have to hire professionals and work with credit bureaus to clear your good name. Identity thieves can use your information to open fraudulent credit card accounts that can show up on your credit report and hurt your credit score. By just monitoring your credit, you could miss certain identity threats. We see more, like if your personal information is used to open a bank account. And if you are a victim, our ID protection helps with identity restoration and even lost wallet coverage.

Exhibit E

***Important Subscription, Pricing and Other Details**

- Your subscription begins when your purchase is completed (or otherwise, when your payment is received). You must download and install on each device, or complete enrollment to be protected. Special offers may expire at any time at NortonLifeLock's discretion.
- By subscribing, you are purchasing a recurring subscription which will automatically renew.
- The price quoted today is valid for the offered introductory term. After that, your subscription will be billed at the applicable monthly or annual renewal price [here](#). The price is subject to change, but we will always alert you a minimum of 30 days in advance.
- You can cancel your subscription term, or by contacting Member Services at 888-888-4545. For more details, please visit the [Refund Policy](#).
- Your subscription may include product, service and/or protection updates and features that may be added, modified or removed subject to the acceptance of the [License and Services Agreement](#).

None can prevent a cybercrime or prevent all identity theft.

† The LifeLock alert network includes a variety of product features and data sources. Although it is very extensive, our network does not cover all transactions at all businesses, so you might not receive a LifeLock alert about single sales.

** Prices vary by state during special promotional periods.

†† Based on an on-line survey of 5,000 US adults conducted by The Harris Poll on behalf of NortonLifeLock, January 2020.

††† Terms Time Monitoring feature includes your home, second home, rental home, or other properties where you have an ownership interest.

†††† In your state, the office that maintains real estate records could be known as a county recorder, register of deeds, clerk of the court, or some other government agency.

[View Privacy Statement | Legal](#)

The LifeLock Brand is part of NortonLifeLock Inc. LifeLock identity theft protection is not available in all countries.

Copyright © 2021 NortonLifeLock Inc. All rights reserved. NortonLifeLock, the NortonLifeLock Logo, the Checkmark Logo, NortonLifeLock, and the LockMeIn Logo are trademarks or registered trademarks of NortonLifeLock Inc. or its affiliates in the United States and other countries. Firefox is a trademark of Mozilla Foundation. Android, Google Chrome, Google Play and the Google Play logo are trademarks of Google, LLC. Mac, iPhone, iPad, Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. Alexa and a related logo are trademarks of Amazon.com, Inc. or its affiliates. Microsoft and the Windows logo are trademarks of Microsoft Corporation in the U.S. and other countries. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License. Other names may be trademarks of their respective owners.

Get discounts, info, protection tips, and more

Sign up for promotional emails

Enter Email

We use the information you provide in accordance with our [Privacy Statement](#).

COMPANY

- About
- Blog
- Careers
- For Good
- Investors
- News Room
- Affiliates
- Security
- Sitemap

HELP

- Contact
- Legal information
- Accessibility Policy
- Member Support Center
- Reviews
- Global Privacy Statement
- License and Services Agreement
- Renewal Pricing
- Cancellation and Refund Policy
- Identity Theft Recovery
- What is Identity Theft

BUSINESS SOLUTIONS

- Overview
- Partners
- Employee Benefits
- Data Breach Services



The LifeLock Brand is part of NortonLifeLock Inc. LifeLock identity theft protection is not available in all countries.

Copyright © 2021 NortonLifeLock Inc. All rights reserved. NortonLifeLock, the NortonLifeLock Logo, the Checkmark Logo, NortonLifeLock, and the LockMeIn Logo are trademarks or registered trademarks of NortonLifeLock Inc. or its affiliates in the United States and other countries. Firefox is a trademark of Mozilla Foundation. Android, Google Chrome, Google Play and the Google Play logo are trademarks of Google, LLC. Mac, iPhone, iPad, Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. Alexa and a related logo are trademarks of Amazon.com, Inc. or its affiliates. Microsoft and the Windows logo are trademarks of Microsoft Corporation in the U.S. and other countries. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License. Other names may be trademarks of their respective owners.



Privacy Settings