

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

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

WILLIAM BASS JR., an individual and
California resident, and STEPHEN
ADKINS, an individual and Michigan
resident, on behalf of themselves and all
others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

No. C 18-05982 WHA (JSC)
Consolidated Cases:
No. C 18-06022 WHA (JSC)
No. C 19-00117 WHA (JSC)

**ORDER GRANTING IN PART
AND DENYING IN PART
MOTION TO DISMISS**

INTRODUCTION

In this data-breach putative class action, defendant Facebook, Inc. moves to dismiss the consolidated complaint pursuant to Rule 12(b)(1) and Rule 12(b)(6). The motion to dismiss is **GRANTED IN PART AND DENIED IN PART.**

STATEMENT

1. FACEBOOK, INC.

Defendant Facebook, Inc. operates an online social network where users stay in touch with family and friends, share their thoughts, and connect with each other (Dkt. No. 76 ¶¶ 1, 9–11). This primarily happens on the user’s “Timeline” — a space to share experiences by

1 posting various forms of content, such as comments, photos, and videos (Bream Decl. ¶¶ 7, 8).
2 Facebook’s platform is widely used throughout the world. Facebook has approximately 2.2
3 billion users and an annual revenue of \$40.65 billion (Dkt. No. 76 ¶¶ 1, 11).

4 Facebook primarily generates its revenue by monetizing its users’ information. None
5 of its 2.2 billion users pay Facebook money (*id.* ¶ 10). Instead, approximately 96% of
6 Facebook’s revenue “originate[s] from the sale of targeted advertising based on the extensive
7 data Facebook collects, analyzes, and maintains about its users” (*id.* ¶ 11). In addition, the
8 collected information enables the platform technology to operate (*id.* ¶¶ 26, 28, 32).

9 At minimum, Facebook requires every user to share their “name, email address or
10 mobile phone number, date of birth, and gender” (*id.* ¶ 26). In full, however, Facebook
11 purportedly collects a much broader set of data, including:

12 all posts, photos and videos, all replies, likes and reactions,
13 all friends and friend history, all games, every “follow”
14 including individuals, event, activity, service, application,
15 group, web sites, advertisements, all followers of the same,
16 all messages exchanges, event RSVPs, all profile
17 information (username, devices, authentication methods,
18 recoverable email accounts and credentials, encryption
19 settings, phone numbers, challenge response information,
20 biometric information and settings, birth date, major
21 events, employment, education, education history, personal
22 preferences, “about me,” religion and political preferences,
23 work history, book preferences, fitness data, news feed
24 preferences, musical preferences), GPS locations where
25 messages, photos, and posts were made, all “pokes,” all
26 advertisements, all calls and messages and associated event
27 logs, and all security and login information including all
28 devices used to access Facebook.

21 (*id.* ¶ 126).

22 The collection and maintenance of all this information has impelled Facebook to provide
23 some transparency as to its data-protection practices. To this end, two separate links posted on
24 the website, entitled “Data Policy” and “Privacy Basics” contain representations as to what data
25 are collected, what data are shared, and with whom (*id.* ¶¶ 38, 44). The links also include
26 certain representations such as “Privacy Principles” where Facebook asserts “[w]e design
27 privacy into our products from the outset,” “[w]e work around the block [sic] to help protect
28 people’s accounts,” and “[w]e are accountable” (*id.* ¶ 44).

1 Nevertheless, Facebook users’ private information has not been protected. In 2007,
 2 Facebook’s then-57 million users settled a class action suit which arose from Facebook’s
 3 “privacy” practices for \$9.5 million. The following year, Facebook exposed the birthdays of
 4 roughly 80 million users (*id.* ¶¶ 11, 47–50). Then, in 2011, Facebook settled with the Federal
 5 Trade Commission over charges that it had deceived users by “telling them they could keep
 6 their information on Facebook private, and then repeatedly allowing it to be shared and made
 7 public” (*id.* ¶ 54 n.32) (quoting *Facebook Settles FTC Charges that it Deceived Consumers by*
 8 *Failing to Keep Privacy Promises*, The Fed. Trade Comm’n (Nov. 29, 2011),
 9 <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceive>
 10 [dconsumers-failing-keep](https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceive)). More recently, in 2015, the world learned that Cambridge Analytica
 11 had misused personal data from Facebook to generate targeted political advertisements.
 12 Facebook’s relationship with Cambridge Analytica led to a political uproar. All this preceded
 13 the instant suit (Dkt. No. 76 ¶¶ 48, 58).

14 2. ACCESS TOKENS

15 “Access tokens” star in the instant data breach. When a Facebook user logs into
 16 Facebook with a specific username and password, that user can conveniently access Facebook
 17 again without being forced to re-enter that information. This ease-of-access is facilitated by the
 18 “access token” generated by Facebook for that user upon his or her first log-in. The access
 19 token operates as an automatic super password — an electronic object embedded with all of a
 20 users’ security information — which allows a user to log in numerous times without typing out
 21 their username and password each time. Many companies, not just Facebook, use this tool to
 22 reduce barriers between the user and the online platform thereby increasing ease-of-access and
 23 efficiency (*id.* ¶¶ 81–83).

24 Facebook’s access tokens, however, carry specific value. As stated in the consolidated
 25 complaint:

26 [o]nce a malicious actor is able to gain access to and
 27 compromise that user’s access token, Facebook’s lack of
 28 security and safeguards allowed that malicious actor to then
 use that access token to gain access to and compromise all
 tokens from that user’s shared or connected web
 applications (i.e., those applications that utilize the

1 “Facebook Login” system, such as Microsoft Azure cloud
 2 platform, Salesforce, etc.). Worse, that malicious actor
 3 could then reset all user permissions, passwords, and other
 4 safeguards (such as two-factor authentication) *not only in*
 5 *Facebook, but also any third-party accounts that utilize*
 6 *Facebook’s authentication login features and do so in such*
 7 *a manner that the user is not provided an alert or any other*
 8 *notification.* From there, the malicious actor can syphon
 [sic] PII and other personal data from those accounts
 without hindrance. To prevent unauthorized users from
 eavesdropping, there is free software to validate the data
 transferred between the client browser and the application
 servers. Most hackers also utilize the free software as a
 simple method to detect and identify easy areas of exploit.

9 (*Id.* ¶ 110) (emphasis added).

10 Put simply, once a Facebook user’s access token is compromised, all tokens from the
 11 user’s shared or connected web applications (like Skype and Uber) purportedly become
 12 accessible. In addition, anyone with access to the token can reset all other user data permissions
 13 and steal the tokens of all connected applications without alerting the original user. Facebook’s
 14 access tokens are allegedly the key to a breathtaking amount of online access (*id.* ¶¶ 99–101,
 15 109).

16 Importantly, standard industry practice is for companies to limit the lifespan of the
 17 tokens. By contrast, Facebook allegedly designed its access tokens to never expire (*id.* ¶¶ 83,
 18 106–109). With this background in tow, this order now turns to the events at issue.

19 **3. THE DATA BREACH**

20 On September 14, 2018, Facebook discovered it had a coding vulnerability related to its
 21 “View As” feature. The vulnerability revealed users’ access tokens. Hackers accordingly stole
 22 the access tokens for 69,000 users. This led to the theft of a narrow set of information for 15
 23 million worldwide users (2.7 million United States users) and a more comprehensive set of
 24 information for 14 million worldwide users (1.2 million United States users) (*id.* ¶¶ 84, 95).

25 The hacking began sometime after July 2017. The specific source of the vulnerability
 26 related to the internal coding of Facebook’s “View As” feature. This feature permitted users to
 27 see what their own “Timeline” looked like to other users (*id.* ¶¶ 3, 88, 91, 94). To illustrate, if a
 28 teenage user wanted to see his own account from the perspective of his parents’ account, the
 teenager would utilize this “View As” feature *on his own account* to “view” the account “as”

1 his parents. This would enable the teenager to see firsthand what information his parents could
2 and could not see on the teenager's account.

3 Momentarily stepping outside the consolidated complaint, Facebook has provided a
4 declaration with step-by-step information of how the attack took place. Per the declaration,
5 when a user's "Timeline" would be accessed in the "View As" mode, an access token of *the*
6 *other user* would generate in the Hypertext Markup Language ("HTML") of the web page. The
7 HTML is the part of the webpage that says "www.Facebook.com." So, when the teenager
8 viewed his account through the eyes of his parents' account, his parents' access token generated
9 in the part of the webpage that says "www.Facebook.com." These attackers could then utilize
10 the parents' access token to access the parents' account and repeat the identical process with the
11 parents' friends. Ultimately, per Facebook's declaration, approximately 69,000 user accounts
12 had their full accounts accessed through this vulnerability (Bream Decl. ¶¶ 12, 14).

13 This vulnerability did not occur every time a user utilized the "View As" feature.
14 Rather, the vulnerability only materialized if two additional (somewhat random) conditions
15 were satisfied. *First*, the teenager's birthday had to be visible on the "Timeline." *Second*, at
16 least three other users had to have posted birthday messages on that "Timeline" (*id.* ¶¶ 13, 14).

17 Significantly, the vulnerability allowed for access tokens to be generated only if the
18 "seed user" (the teenager) met the conditions described above. Accordingly, even if one user
19 was vulnerable, not every account linked was also vulnerable (*id.* ¶ 16). To illustrate, if the
20 teenager had his birthday visible on his "Timeline" and had three friends wish him happy
21 birthday on his "Timeline," then his parents' access token would be generated when the
22 teenager viewed his account through the eyes of his parents' account. With the parents' access
23 token in hand, the attackers could then turn to the parents' account and treat that account as a
24 new seed user account. If, however, the parents' account did not have a birthday visible on
25 their own "Timeline," the access tokens to the parents' friends' accounts would not be revealed.
26 This would end that branch of the access-token collection tree.

27 The information taken in the attack did not end with these 69,000 users. Facebook
28 connects users to each other. This means that once accounts have been connected to each other

1 as “friends” on Facebook, one user can see another user’s information. Once the attackers
2 compromised the access tokens to an account, account-information associated with connected
3 accounts could be culled as well. This resulted in 29 million users (approximately 4 million
4 users in the United States) having information taken in this data breach, according to Facebook
5 (*id.* ¶ 9).

6 These 29 million users can be divided into two groups. The first group comprises of
7 approximately 15 million users (2.7 million users in the United States). For these users, the
8 attackers obtained solely the user’s name and basic contact information (phone number and/or
9 email addresses, depending on which users had chosen to provide to Facebook) (*id.* ¶ 11.c.).

10 The second group comprises of approximately 14 million users (1.2 million users in the
11 United States). For these users, in addition to the information listed for the first group, the
12 hackers also obtained the username, gender, date of birth, and (if users had chosen to share it)
13 workplace, education, relationship status, religious views, hometown, self-reported current city,
14 website, the user’s locale/language, the types of devices used to access Facebook, the last ten
15 places the user “checked into” or was “tagged” in on Facebook, the people or pages that the
16 user “followed” on Facebook, and the user’s fifteen most recent searches using the Facebook
17 search bar (*id.* ¶ 11.d.).

18 5. THIS ACTION

19 Facebook first became aware of a potential data breach on September 14, 2018.
20 Facebook’s engineering team isolated the security flaws on September 25, 2018. Facebook
21 notified potentially affected users on September 28, 2018. Facebook then purportedly
22 invalidated the access tokens of over 90 million accounts that were potentially impacted by the
23 vulnerability and effected a “forced logout” which “requir[ed] [users] to reenter their
24 passwords” to access their accounts (Dkt. No. 76 ¶¶ 84–87, 91–92).

25 After the breach had been publically announced, eleven separate lawsuits were filed
26 against Facebook. These lawsuits generally alleged that Facebook failed to adequately protect
27 its users’ accounts. A public tutorial on the issue of personal information in the context of data
28 breaches proceeded in the district court. The eleven actions were then consolidated and an

1 amended consolidated complaint was filed (Dkt. Nos. 67, 76). Five named plaintiffs filed the
2 consolidated complaint. Except for one original named plaintiff, every named plaintiff who had
3 not filed the consolidated complaint voluntarily withdrew without prejudice (Dkt. Nos. 87–94).

4 The consolidated complaint asserted ten claims on behalf of a class of Facebook users in
5 the United States “whose [personal identifiable information] was compromised in the data
6 breach announced by Facebook on September 28, 2018” (*id.* ¶¶ 13, 179). Those ten claims are:
7 (i) breach of contract; (ii) breach of implied contract; (iii) breach of implied covenant of good
8 faith and fair dealing; (iv) quasi-contract for non-restitutionary damages; (v) negligence; (vi)
9 negligence per se; (vii) violation of California’s Unfair Competition Law; (viii) violation of
10 California’s Consumer Legal Remedies Act; (ix) breach of confidence; and (x) declaratory
11 judgment.

12 Due to the number of consolidated cases, an order was issued appointing co-interim
13 class counsel to coordinate motion practice and discovery (Dkt. No. 79). Facebook moved to
14 dismiss (Dkt. No. 96). After full briefing (Dkt. Nos. 108, 115), a hearing followed in May
15 2019. At the hearing, it came to light that Facebook had asked for, and not received, the benefit
16 of plaintiffs’ depositions. Those depositions were immediately ordered.

17 The depositions took place. The parties filed supplemental briefing (Dkt. Nos. 122,
18 135). Three of the five remaining named plaintiffs abruptly withdrew (Dkt. Nos. 140–142).
19 This order follows.

20 ANALYSIS

21 Facebook moves under two different rules: Rule 12(b)(1) and Rule 12(b)(6). This order
22 assesses each in turn.

23 1. RULE 12(b)(1)

24 Rule 12(b)(1) requires dismissal of claims where a plaintiff fails to establish subject-
25 matter jurisdiction. *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). “Rule 12(b)(1) attacks
26 on jurisdiction can be either facial, confining the inquiry to allegations in the complaint, or
27 factual, permitting the court to look beyond the complaint.” *Savage v. Glendale Union High*
28 *School, Dist. No. 205, Maricopa County*, 343 F.3d 1036, 1039 n.2 (9th Cir. 2003) (citation

1 omitted). Facebook urges both. Still, because the moving party in a factual attack *converts* the
2 motion into a factual motion, *see Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir.
3 2004), the *facial* attack is subsumed by the *factual* attack. This order therefore only assesses
4 Facebook’s factual attack. We look beyond the complaint.

5 Two named plaintiffs remain in this action — plaintiff Stephen Adkins and plaintiff
6 William Bass. They both allege four theories of harm due to Facebook’s alleged inadequate
7 safeguarding of its users’ personal information. Facebook has factually attacked plaintiffs’
8 Article III standing by properly presenting the declaration of Christopher Bream, the individual
9 who led the security response to the data breach, and depositions of the named plaintiffs. Both
10 plaintiffs must now defend jurisdiction by “furnish[ing] affidavits or other evidence necessary
11 to satisfy its burden of establishing subject matter jurisdiction.” *Wolfe v. Strankman*, 392 F.3d
12 358, 362 (9th Cir. 2004) (citation omitted). For the reasons stated below, plaintiff Stephen
13 Adkins satisfied his burden to establish Article III standing. Plaintiff William Bass did not.

14 **A. PLAINTIFF STEPHEN ADKINS**

15 A federal court’s subject-matter jurisdiction is limited to “cases” or “controversies.”
16 *Raines v. Byrd*, 521 U.S. 811, 818 (1997). This limitation requires plaintiff to have standing to
17 bring suit. “To establish Article III standing, an injury must be ‘concrete, particularized, and
18 actual or imminent; fairly traceable to the challenged action; and redressable by a favorable
19 ruling.’” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013) quoting (*Monsanto Co. v.*
20 *Geertson Seed Farms*, 561 U.S. 139, 149 (2010)). Plaintiff shoulders the burden to establish
21 these elements “with the manner and degree of evidence required at the successive stages of
22 litigation.” *Lujan v. Def. of Wildlife*, 504 U.S. 555, 561 (1992). Nevertheless, should a plaintiff
23 fail to meet his standing burden, the lawsuit must be dismissed under Rule 12(b)(1). *Steel Co.*
24 *v. Citizens for a Better Env’t*, 523 U.S. 83, 109–110 (1998).

25 The bugaboo here is the first standing element: injury in fact. To satisfy the injury in
26 fact element, “the plaintiff must show that he personally has suffered some actual or threatened
27 injury as a result of the putatively illegal conduct of the defendant.” *Gladstone Realtors v. Vill.*
28 *of Bellwood*, 441 U.S. 91, 99 (1979). “[T]hreatened injury must be certainly impending” and a

1 “possible future injury” does not suffice. *Clapper*, 568 U.S. at 409 (quotations omitted).
2 “[N]amed plaintiffs who represent a class must allege and show that they personally have been
3 injured, not that injury has been suffered by other, unidentified members of the class to which
4 they belong and which they purport to represent.” *Lewis v. Casey*, 518 U.S. 343, 357 (1996)
5 (citations and internal quotations omitted).

6 Plaintiff Adkins alleged the following four harms: (i) substantial risk of future identity
7 theft based on the information taken; (ii) lost time responding to the data breach; (iii) loss of the
8 value of personal information; and (iv) failure to receive the benefit of his bargain with
9 Facebook. The former two harms have been sufficiently established at this stage. It is therefore
10 unnecessary to consider the latter two here. (Because they are economic harms, the latter two
11 alleged harms will instead be analyzed in the context of Section 17200 and the CLRA.)

12 Facebook notified plaintiff Adkins that he had been subject to the data breach. A
13 reasonable inference can therefore be drawn which traces the plausibly alleged harms to the
14 purported mishandling of plaintiff Adkins’s personal information through the data breach.
15 Accordingly, at this stage, plaintiff Adkins has established that he has standing.

16 Plaintiff Adkins provided Facebook with his name, email address, telephone number,
17 date of birth, locations, work and education history, hometown, relationship status, and
18 photographs (Adkins Dep. 185:2–186:10, 314). Facebook informed plaintiff Adkins through a
19 notification that his information had been taken in this data breach. Plaintiff Adkins purported
20 to have subsequently received extensive “phishing” emails and text messages. Plaintiff Adkins
21 also spent as much as an hour managing the aftermath of the data breach (Dkt. No. 76 ¶¶
22 163–170). This order now assesses the dual harms of risk of future identity theft and lost time.

23 *i. Risk of Future Identity Theft*

24 The information taken in this data breach gave hackers the means to commit further
25 fraud or identity theft. Plaintiff Adkins personally alleges this information was taken.
26 Specifically, his name, email address, telephone number, date of birth, locations, work and
27 education history, hometown, relationship status, and photographs now reside with criminals
28 (Adkins Dep. 185:2–186:10, 314). Extensive “phishing” emails and text messages have

1 bombarded plaintiff Adkins since the attack. Between the hacking and the phishing, plaintiff
2 Adkins has plausibly shown risk of further fraud and identity theft.

3 Facebook argues that no sensitive information was taken. In *Krottner v. Starbucks*
4 *Corp.*, our court of appeals concluded that the combination of the sensitivity of personal
5 information with its theft can suffice to allege injury-in-fact. 628 F.3d 1139, 1140–43 (9th Cir.
6 2010). There, some of the data taken included social security numbers. Here, Facebook has
7 gone to great lengths to show that all the information taken was otherwise publicly available
8 information and not sensitive.

9 The information taken, however, need not be sensitive to weaponize hackers in their
10 quest to commit further fraud or identity theft. To this end, a more recent decision from our
11 court of appeals held that the rightful injury-in-fact determination is not to look at the minutia of
12 what information had been taken — such as credit card information or social security numbers
13 — but to specifically determine whether the data taken “gave hackers the means to commit
14 fraud or identity theft.” *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027–29 (9th Cir. 2018), *cert.*
15 *denied sub nom. Zappos.com v. Stevens*, 139 S. Ct. 1373 (2019). This is not a departure from
16 *Krottner*, which emphasized that the key inquiry was the “increased risk of identity theft.”
17 *Krottner*, 628 F.3d at 1142. Imminent injury in fact can be established through information
18 similar in function to social security numbers so long as the stolen data operated to be
19 “sufficiently similar to that in *Krottner* to require the same conclusion” *In re Zappos.com,*
20 *Inc.*, 888 F.3d at 1027.

21 The stolen data here is sufficiently similar. A social security number derives its value in
22 that it is immutable. So is someone’s date of birth, hometown, and high school, which had been
23 taken here from plaintiff Adkins. As a result of this data breach, this information can now
24 forever be wielded to identify plaintiff Adkins and target him in fraudulent schemes and identity
25 theft attacks. The rest of the alterable information taken, such as plaintiff Adkins’s name, email
26 address, telephone number, locations, work and education history, relationship status, and
27 photographs, now in the hands of nefarious actors, will provide further ammo. Put simply, the
28

1 amount of information taken “gave hackers the means to commit fraud or identity theft.” *Ibid.*
2 This suffices under *Krottner* and *Zappos*.

3 We must not forget that the hackers did not merely attack Facebook and loot it. These
4 hackers went out of their way to run search queries on 69,000 hacked accounts for the sole
5 purpose of culling personal information from an additional 30 million people. The attackers’
6 cards have been revealed: the goal was not merely to attack, the goal was to take personal
7 information on a mass scale. It is not too great a leap to assume, therefore, that their goal in
8 targeting and taking this information was to commit further fraud and identity theft.

9 That each strand of information can be painstakingly collected through a mishmash of
10 other sources is irrelevant. Facebook is a centralized location which stores personal information
11 for billions of users. Constructing this information from random sources bit by bit, would be
12 hard.

13 “Where a data breach targets personal information, a reasonable inference can be drawn
14 that the hackers will use the victims’ data for the fraudulent purposes alleged in Plaintiffs’
15 complaints.” *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 388 (6th Cir. 2016).
16 “Why else would hackers break into a store’s database and steal consumers’ private
17 information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent
18 charges or assume those consumers’ identities.” *Remijas v. Neiman Marcus Grp., LLC*, 794
19 F.3d 688, 693 (7th Cir. 2015). Between the obvious goal of taking personal information, the
20 nature and amount of information taken, and the extended phishing emails which have
21 subsequently followed the attack, plaintiff Adkins has plausibly shown he is at risk of further
22 fraud and identity theft.

23 *ii. Loss of Time*

24 Our court of appeals has never considered whether loss of time rectifying the aftermath
25 of a data breach suffices to establish harm for standing. Recently, however, the United States
26 Court of Appeals for the Seventh Circuit stated that in a data breach, “the value of one’s own
27 time needed to set things straight is a loss from an opportunity-cost perspective.” *Dieffenbach*
28 *v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018). Here, plaintiff Adkins has stated

1 that he received around 30 e-mails which he spent between a few minutes and an hour sorting
 2 through (Adkins Dep. 204:9–205:2). This order agrees with *Dieffenbach* that loss of time
 3 establishes injury in fact.

4 This order also concludes that the amount of time alleged here establishes injury. True,
 5 sorting through a few dozen e-mails may or may not have taken an hour to rectify and perhaps
 6 the time spent later proves *de minimis*. This story, however, has yet to end. As consequences
 7 of this data breach continue to unfold, so too, will plaintiff’s invested time. More phishing e-
 8 mails will pile up. At this stage, the time loss alleged suffices.

9 * * *

10 Plaintiff Adkins has established standing through the dual harms of increased risk of
 11 future harm and loss of time. As to plaintiff Adkins, Facebook’s Rule 12(b)(1) motion is
 12 therefore **DENIED**.

13 **B. PLAINTIFF WILLIAM BASS, JR.**

14 At the pleading stage, plaintiff bears the burden of “demonstrating that . . . injury-in-fact
 15 is . . . fairly traceable to the challenged action.” *Davidson v. Kimberly-Clark Corp.*, 889 F.3d
 16 956, 967 (9th Cir. 2018), *cert. denied*, 129 S. Ct. 640 (2018) (citing *Monsanto Co. v. Geertson*
 17 *Seed Farms*, 561 U.S. 139, 149 (2010)). Here, the challenged action is Facebook not
 18 adequately safeguarding its users’ personal information. Plaintiff Bass’s allegations do not
 19 demonstrate a plausible link to that action.

20 The main difference between plaintiff Bass and plaintiff Adkins in terms of establishing
 21 standing, is that plaintiff Adkins alleged he received a notification from Facebook informing
 22 him that he had been a victim of the data breach, thereby connecting him to the data breach.
 23 Plaintiff Bass never so alleges. Of course, the lack of a notice alone does not foreclose plaintiff
 24 Bass from establishing standing. What forecloses plaintiff Bass from establishing standing here
 25 is that none of the circumstantial evidence he provides plausibly connects to the data breach.
 26 Either the facts do not trace to the data breach at all or are so common the infinite possibilities
 27 forecloses plausibility. Plaintiff Bass has not met his burden.

28

1 Plaintiff Bass alleges he was a victim of the data breach because of three facts: (i) he had
2 been forcibly logged out of his Facebook account; (ii) he received phone calls from people
3 purporting to be his family members; and (iii) he subsequently received fake Facebook friend
4 requests, spam e-mails, and pornographic links on his Facebook messenger service.

5 These allegations do not suffice to connect the dots to the data breach. The first two
6 facts do not trace to the data breach at all. The consolidated complaint provided that Facebook
7 logged 90 million users out of their accounts to re-set access tokens (Dkt. No. 76 ¶ 4).
8 Accordingly, the data breach did not cause the log-outs, Facebook's independent action did. It
9 is also impossible to tell why plaintiff Bass assumed the phone calls materialized as a result of
10 the data breach. The calls began in late August or early September (Bass Dep. 57:18–23). This
11 was well before personal information from the data breach began to leak. Zero evidence
12 demonstrates that hackers (or their customers) call their victims purporting to be family. No
13 reasonable inference can be drawn connecting the log-outs and these calls to the data breach.

14 As to the third alleged fact, spam e-mails and fake friend requests simply occur to most,
15 if not all, e-mail and social media users. They are too common and therefore cannot on their
16 own establish causation here. To hold otherwise would effectively negate the standing
17 requirement as to data breaches. Accordingly, although these occurrences may be evidence of
18 having been the victim of a data breach, *on their own*, they cannot serve to connect plaintiff
19 Bass to the data breach.

20 To reiterate, that Facebook did not notify plaintiff Bass that he had been victimized by
21 the data breach does not foreclose a plausible allegation at this early stage. Still, *some* plausible
22 connection to the data breach must be shown. Plaintiff Bass cannot merely assume he was a
23 victim through facts that do not trace to the data breach and through occurrences so common the
24 link to the data breach is merely possible.

25 Real victims from this data breach exist. Facebook has put forward sufficient evidence
26 to show that plaintiff Bass was not one of them. Plaintiff Bass has not sufficiently rebutted this
27 evidence. Facebook's Rule 12(b)(1) motion as to plaintiff Bass is **GRANTED**.

28

1 **2. RULE 12(b)(6)**

2 To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain sufficient
3 factual matter, accepted as true, to state a claim for relief that is plausible on its face. *Ashcroft*
4 *v. Iqbal*, 556 U.S. 662, 678 (2009). A claim is facially plausible when there are sufficient
5 factual allegations to draw a reasonable inference that defendants are liable for the misconduct
6 alleged. While a court must take all of the factual allegations in the complaint as true, it is “not
7 bound to accept as true a legal conclusion couched as a factual allegation.” *Bell Atl. Corp. v.*
8 *Twombly*, 550 U.S. 544, 555 (2007).

9 **A. LIMITATION-OF-LIABILITY SHOWSTOPPER**

10 The limitation-of-liability clause stops five alleged claims from moving forward. These
11 claims are: (i) breach of contract, (ii) implied contract, (iii) implied covenant of good faith and
12 fair dealing, (iv) quasi-contract, and (v) breach of confidence.

13 The Terms of Service provide that California law governs both the terms and any claim.
14 Perhaps regrettably, “[w]ith respect to claims for breach of contract, limitation of liability
15 clauses are enforceable unless they are unconscionable, that is, the improper result of unequal
16 bargaining power or contrary to public policy.” *Food Safety Net Servs. v. Eco Safe Sys. USA,*
17 *Inc.*, 209 Cal. App. 4th 1118, 1126 (2012). Specifically, the Terms of Service covered use of
18 Facebook.com. The limitation-of-liability clause contained therein provided:

19 [w]e work hard to provide the best Products we can and to
20 specify clear guidelines for everyone who uses them. Our
21 Products, however, are provided “as is,” and **we make no**
22 **guarantees that they always will be safe, secure, or**
23 **error-free**, or that they will function without disruptions,
24 delays, or imperfections. . . . We do not control or direct
what people and others do or say, and **we are not**
responsible for their actions or conduct (whether online
or offline) or any content they share (including offensive,
inappropriate, obscene, unlawful, and other objectionable
content).

25 We cannot predict when issues might arise with our
26 Products. **Accordingly, our liability shall be limited to**
27 **the fullest extent permitted by applicable law**, and under
28 no circumstance will we be liable to you for any lost
profits, revenues, information, or data, or consequential,
special, indirect, exemplary, punitive, or incidental
damages arising out of or related to these Terms or the
Facebook Products, even if we have been advised of the

possibility of such damages. Our aggregate liability arising out of or relating to these Terms or the Facebook Products will not exceed the greater of \$100 or the amount you have paid us in the past twelve months.

(Dkt. No. 98, Exh. A at Sec. 4.3) (emphasis added). The “applicable law” within the meaning of the second paragraph quoted above is California Civil Code Section 1668, which established that:

All contracts which have for their object, directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law.¹

Accordingly, the only way the breach of contract claims may move forward is if the limitation-of-liability clause is deemed unconscionable. *Food Safety Net Servs.*, 209 Cal. App. at 1126. “[U]nconscionability has both a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided results.” *Mohamed v. Uber Techs., Inc.*, 848 F.3d 1201, 1210 (9th Cir. 2016) (internal quotation marks and citations omitted). The ultimate issue is whether, in view of all relevant circumstances, the contract is so unfair that enforcement must be withheld.

Facebook is not cost-free. The user incurs the cost of having his information mined and shared. Even if this is not a monetary charge, the user still incurs this burden. Nonetheless, the procedure followed by Facebook was fair. The clause was not buried. The clause was plainly above board and contained clear enough language. True, it is an adhesion contract, but there is no “rule that an adhesion contract is per se unconscionable.” *Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1261–62 (9th Cir. 2017). No one is forced to enroll in Facebook’s social media service. The four breach-of-contract claims are therefore dismissed. The breach of confidence claim is also dismissed because it is covered by the clause.

* * *

¹ The Terms of Service was linked to, but not specifically quoted, in the consolidated complaint. Nonetheless, the consolidated complaint relied on the Terms of Service at length to allege its breach of contract claims and statutory claims. As such, Facebook’s request to incorporate by reference the Terms of Service (Dkt. No. 99, Exh. A) is **GRANTED**.

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

1 Facebook next argues that the limitation-of-liability clause should be a showstopper for
2 negligence and negligence per se as well. As an aside, “under California law, negligence per se
3 is a doctrine, not an independent cause of action.” *Dent v. Nat’l Football League*, 902 F.3d
4 1109 (9th Cir. 2018) citing (*Quiroz v. Seventh Ave. Ctr.*, 140 Cal. App. 4th 1256 (2006)). These
5 two alleged claims are therefore only one claim. Collapsing both alleged claims into one claim,
6 this order allows the negligence claim to proceed.

7 “An agreement insulating one from liability for his own negligence must specifically so
8 provide and is strictly construed against the party asserting the exemption, especially where he
9 is the author of the agreement.” *Viotti v. Giomi*, 230 Cal. App. 2d 730, 739 (1964). “An
10 agreement which seeks to limit generally without mentioning negligence is construed to shield a
11 party only for passive negligence, not for active negligence.” *Burnett v. Chimney Sweep*, 123
12 Cal. App. 4th 1057, 1066 (2004) (quotations omitted). “Whereas passive negligence involves
13 mere nonfeasance, such as the failure to discover a dangerous condition or to perform a duty
14 imposed by law, active negligence involves an affirmative act, *knowledge of or acquiescence in*
15 *negligent conduct*, or failure to perform specific duties.” *Frittelli, Inc. v. 350 N. Canon Drive,*
16 *LP*, 202 Cal. App. 4th 35, 48 (2011) (quotation omitted) (emphasis added). In other words,
17 Facebook’s mere failure to discover the vulnerability might be barred by the clause, but if it had
18 acquiesced to, or known of the vulnerability, the claim would certainly be allowed through.

19 Here, the limitation-of-liability clause does not mention “negligence” at all, let alone
20 unequivocally preclude liability for negligence. At this early stage, no facts have been teased
21 out. Precluding the claims for negligence pursuant to the liability clause is therefore
22 impossible. They remain for now.

23 B. CLAIM FOR NEGLIGENCE

24 This order now turns away from the limitation of liability and considers whether a claim
25 for relief based on negligence has been adequately pled.

26 This order holds that negligence has been plausibly alleged. To state a claim for
27 negligence in California, a plaintiff must establish the following elements: (1) the defendant had
28 a duty, or an “obligation to conform to a certain standard of conduct for the protection of others

1 against unreasonable risks,” (2) the defendant breached that duty, (3) that breach proximately
2 caused the plaintiff’s injuries, and (4) damages. *Corales v. Bennett*, 567 F.3d 554, 572 (9th Cir.
3 2009) quoting *McGarry v. Sax*, 158 Cal. App. 4th 983 (2008). The consolidated complaint
4 plausibly alleged each of these elements.

5 Specifically, Facebook allegedly failed to comply with minimum data-security standards
6 during the period of the data breach. For example, “[i]ndustry-standard information and data
7 security best practices demand that companies that utilize access tokens should limit the
8 lifespan of those access tokens to a reasonable period (e.g., an hour, a day, a week, a month)”
9 (Dkt. No. 76 ¶ 82). In turn, this breach plausibly caused the harm to plaintiff resulting in
10 alleged damages. This is a classic negligence claim.

11 Facebook argues it does not owe its users a duty of care. California courts consider
12 several factors when deciding whether a duty of care exists, including “the foreseeability of
13 harm to the plaintiff, the degree of certainty that the plaintiff suffered injury, the closeness of
14 the connection between the defendant’s conduct and the injury suffered, the moral blame
15 attached to the defendant’s conduct, the policy of preventing future harm, the extent of the
16 burden to the defendant and the consequences to the community of imposing a duty to exercise
17 care with resulting liability for breach, and the availability, cost, and prevalence of insurance for
18 the risk involved.” *Regents of Univ. of Cal. v. Superior Court*, 4 Cal. 5th 607, 628 (2018)
19 (quoting *Rowland v. Christian*, 69 Cal. 2d 108 113 (1968)). These factors “must be evaluated at
20 a relatively broad level of factual generality.” *Ibid.* (quotation omitted).

21 These factors have been satisfied here. The lack of reasonable care in the handling of
22 personal information can foreseeably harm the individuals providing the information. Further,
23 some of the information here was private, and plaintiff plausibly placed trust in Facebook to
24 employ appropriate data security. From a policy standpoint, to hold that Facebook has no duty
25 of care here “would create perverse incentives for businesses who profit off the use of
26 consumers’ personal data to turn a blind eye and ignore known security risks.” *In re Equifax,*
27 *Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019) (Judge
28

1 Thomas Thrash). As such, plaintiff Adkins has met his obligation to plausibly plead duty of
2 care.

3 Finally, Facebook argues that the economic loss rule bars plaintiff's negligence claim.
4 Generally, purely economic losses are not recoverable in tort. *Seely v. White Motor Co.*, 63 Cal.
5 2d 9, 16–17 (1965). Put simply, “the economic loss rule prevent[s] the law of contract and the
6 law of tort from dissolving one into the other.” *Robinson Helicopter Co., v. Dana Corp.*, 34
7 Cal. 4th 979, 988 (2004) (quotation omitted). The rule serves to “limit liability in commercial
8 activities that negligently or inadvertently go awry.” *Id.* at 991 n.7. Here, plaintiff alleged his
9 loss of time as a harm and so does not allege pure economic loss. The economic loss rule
10 therefore does not apply.

11 C. CLAIMS UNDER SECTION 17200 AND THE CLRA

12 In order to establish standing for Section 17200 and the CLRA, plaintiffs must show that
13 they personally lost money or property “as a result of the unfair competition.” Cal. Bus. & Prof.
14 Code § 17204; *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 330 (2011). “There are
15 innumerable ways in which economic injury from unfair competition may be shown. A
16 plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she
17 otherwise would have; (2) have a present or future property interest diminished; (3) be deprived
18 of money or property to which he or she has a cognizable claim; (4) be required to enter into a
19 transaction, costing money or property, that would otherwise have been unnecessary.” *Id.* at
20 323.

21 Plaintiff Adkins alleged two harms, which if plausible, would satisfy this criteria:
22 (i) loss of the value of the personal information and (ii) failure to receive the benefit of his
23 bargain with Facebook. Neither harm has been plausibly alleged.

24 As to the loss of value of the personal information, plaintiff Adkins has provided no
25 market for the personal information or the impairment of the ability to participate in that
26 market. This lack of specificity is fatal. It is not enough to merely say the information was
27 taken and therefore it has lost value. In addition, plaintiff Adkins has not shown how this
28 information has economic value *to him*. That the information has external value, but no

1 economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or
2 property.

3 Turning to the second alleged economic harm, plaintiff Adkins alleged that he had given
4 over his personal information with the bargain that the information would be secure. The
5 information was not secure and therefore he lost the benefit of his bargain. Yet, even if plaintiff
6 Adkins did intend to sell his own data — an intention he did not have — it is unclear whether or
7 how the data has been devalued by the breach. This alleged economic harm therefore also fails.

8 * * *

9 Plaintiff Adkins has only plausibly alleged harm arising from risk of future harm and
10 loss of time. As alleged, neither of these show “lost money or property as a result of the unfair
11 competition.” Cal. Bus. & Prof. Code § 17204. Accordingly, plaintiff Adkins has not
12 sufficiently alleged standing under Section 17200 and the CLRA.

13 **D. DECLARATORY JUDGMENT**

14 Plaintiff seeks a declaratory judgment that Facebook’s existing security measures do not
15 comply with its explicit or implicit contractual obligations to provide adequate security, and
16 duties of care towards plaintiff’s personal identifiable information. A dispute exists as to the
17 continued risk plaintiff Adkins and similarly situated Facebook users face. While Facebook
18 purports to have fixed the issues which led to this data breach, it is too early in the litigation to
19 confidently say whether that is so. Dismissal of the declaratory judgment relief would be
20 premature here.²

21 **CONCLUSION**

22 To the extent stated, the motion to dismiss is **GRANTED IN PART AND DENIED IN PART**.
23 Only plaintiff Adkins may proceed with his claims. Plaintiff Bass has not adequately alleged
24 standing. For plaintiff Bass to proceed, he must specify a connection to the data breach. Leave
25 to amend will be allowed for him to attempt to do so.

26 * * *

27 _____
28 ² The request for incorporation by reference by Facebook of the *Privacy Basics* website (Dkt. No. 99, Exh. B) and the request for judicial notice by plaintiff Adkins of four Facebook-related privacy webpages (Dkt. No. 108-8) are **DENIED AS MOOT**.

1 Excluding standing, the order holds as follows. *First*, the four breach of contract claims
 2 and the breach of confidence claim cannot move forward because of the limitation-of-liability
 3 clause. Leave to amend will be allowed, however, because facts may conceivably be alleged
 4 which go towards determining whether procedural unfairness existed upon entering into the
 5 contract. *Second*, turning to the next two claims, negligence and negligence per se, these
 6 survive the motion to dismiss as a single claim. The limitation-of-liability clause does not
 7 preclude negligence here because contracts that limit liability without mentioning negligence
 8 specifically narrow the scope of liability based on a severe factual determination. Some
 9 circumstances will bar the claim under the clause. Some will cause the claim to survive the
 10 clause. So, this order takes a discovery-first approach to whether the clause applies to the
 11 negligence claim. Moving past the waiver, negligence has been plausibly alleged. *Third*,
 12 turning to the next two claims, the Section 17200/CLRA claims are barred because the only
 13 harm plaintiff plausibly alleged is risk of future harm and loss of time. Both of these statutes,
 14 however, require economic injury (money/property). Plaintiff Adkins may seek leave to amend.
 15 *Fourth*, the last claim is for declaratory judgment. This claim survives because the rights of the
 16 parties remain unknown at this early stage. In sum, only the dual claims for negligence and
 17 declaratory judgment survive the motion to dismiss. Negligence per se survives as a theory of
 18 the asserted negligence claim but not as a standalone claim. The rest of the claims are
 19 dismissed with leave to amend as set forth below. Discovery should be moving with alacrity.


20 * * *

21 Both plaintiffs may move for leave to amend by **JULY 18** at **NOON**. Any such motion
 22 should include as an exhibit a redlined version of the proposed amendments that clearly
 23 identifies all changes from the initial complaint. This order highlights certain deficiencies in
 24 the initial complaint, but it will not necessarily be enough to add a sentence parroting each
 25 missing item identified herein. If plaintiffs so move, they should be sure to plead their best
 26
 27
 28

1 case. Any motion should explain how the proposed complaint overcomes all deficiencies, even
2 those this order did not reach.

3
4 **IT IS SO ORDERED.**

5
6 Dated: June 21, 2019.

7 
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
WILLIAM ALSUP
UNITED STATES DISTRICT JUDGE