Andrew N. Friedman (*pro hac vice*)
afriedman@cohenmilstein.com
**COHEN MILSTEIN SELLERS & TOLL PLLC**
1100 New York Ave. NW, Fifth Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
**MORGAN & MORGAN**
**COMPLEX LITIGATION GROUP**
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: 813/223-5505
Facsimile: 813/223-5402

Ariana J. Tadler (*pro hac vice*)
atadler@tadlerlaw.com
**TADLER LAW, LLP**
One Penn Plaza
New York, NY 10119
Telephone: (212) 946-9453
Facsimile: (212) 273-4375

*Attorneys for Plaintiff*

**UNITED STATES DISTRICT COURT FOR THE**
**NORTHERN DISTRICT OF CALIFORNIA**
**SAN FRANCISCO DIVISION**

STEPHEN ADKINS, an individual and Michigan resident, on behalf of himself and all others similarly situated,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.

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

**PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFF'S MOTION FOR CLASS CERTIFICATION**

Date: October 31, 2019
Time: 8:00am
Court: Courtroom 12, 19th Floor
Hon. William Alsup

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**CASES**

**STATUTES**

**OTHER AUTHORITIES**

## INTRODUCTION

Defendant Facebook has made billions annually off its global platform. Users provide various forms of personally identifiable information ("PII") that third parties access to target ads. However, Facebook—whose motto was "move fast, break things"[1]—moved too fast and created vulnerabilities to its platform that allowed hackers to steal PII from at least 29 million users worldwide, including more than four million users in the United States. Among the PII looted were class members' names, email addresses, telephone numbers, and for nearly half of the class, work and education history, relationship status, date of birth, hometown, and other historical PII, neatly packaged in a centralized format, providing ease of exploitation. The repercussions of the September 2018 data breach ("Breach") are far-reaching and long-lasting, as, given the sophistication of present-day cybercriminals, PII "need not be sensitive to weaponize hackers in their quest to commit further fraud and identity theft." ECF No. 153 at 10.

Facebook's negligence caused this harm. Facebook ignored known risks when developing its authentication infrastructure by using non-expiring access tokens for users. These functioned like passkeys. While the tokens permitted the user to stay logged on (and user activity yielded more money to Facebook), the tokens also permitted the hackers to intrude upon user profiles without a password or other check to ensure that the person accessing the account and information was an authorized user. Facebook engineers repeatedly discussed the risks of persistent access tokens before the Breach. But Facebook kept using these tokens, putting profits over the risks to PII.

Facebook was also slow to react to the Breach. Facebook's Growth Team—which follows user metrics—first noted a suspicious spike in activity among dormant accounts on approximately September 17, 2018. However, it did not escalate the matter to security personnel until September 25, 2018. This provided ample space for the hackers, who scraped PII from millions of profiles before the Security Team logged off 90 million users to staunch the theft. But by then, 29 million

[1] In 2014, Facebook changed its motto for developers from "Move Fast and Break Things" to "Move Fast With Stable Infra." They feared that may have been moving too fast to see where they were going clearly. With good reason. Oct 19, 2018. https://mindmatters.ai/2018/10/facebooks-old-motto-was-move-fast-and-break-things.

users were hacked. Facebook's failure to responsibly act resulted in millions of users having the value of their PII diminished and having to forever worry about identity theft.

Plaintiff seeks certification of his claims for negligence and declaratory relief, which claims are naturally suited for resolution on a classwide basis. In his Rule 12(b)(1) affidavit, Facebook's security engineering director, Chris Bream, described how the Breach uniformly affected consumers, the groups of consumers involved, and the types of PII released. ECF No. 97. Plaintiff and class members were injured by the same Breach. Because Facebook's data security practices uniformly apply to all class members, common issues will predominate in the trial of all claims arising from the Breach. Class treatment is superior as individual consumers cannot be expected to present the technical documents and expert testimony needed to prove that Facebook knowingly ignored its data security vulnerabilities and belatedly responded to the Breach. Facebook, a 50-billiion-dollar behemoth, has both the means and responsibility to protect its users' PII. Finally, the remedies available to class members will also be common: money towards the reduced value of their PII; money towards credit monitoring; and a list of reforms to prevent future damage. The Court should certify Plaintiff's claims pursuant to Rule 23(b)(2) (as to injunctive relief), 23(b)(3) (as to diminished value and credit monitoring), and/or 23(c)(4) for those who wish to prove out-of-pocket damages.

## FACTUAL BACKGROUND

### A. Facebook Created a Security Vulnerability with NoConfidence Tokens

When a user logs into Facebook with a username and password, Facebook generates an access token for that user.[2] This access token operates as an automatic super password—an all-purpose key mapped to a user's profile—which allows the user to access Facebook without entering

[2] *See* August 29, 2019 Declaration of Douglas J. McNamara is Support of Plaintiff's Motion for Class Certification ("McNamara Decl.") at Ex. 1, FB-SCHMIDT-000054545. References to "Ex." are to exhibits appended to the McNamara Declaration.

a username and password each time.[3] This practice streamlines logins and reduces the barriers for users to access the Facebook platform—but also creates risks.[4]

Since at least 2017, Facebook has used "NoConfidence" tokens, which give the individual deploying them a high level of permissible actions but provide no verification that the person using the token is the one who originally entered the username and password to generate it.[5] NoConfidence tokens do not require an end user's credentials and will even bypass multi-factor authentication.[6] Among the NoConfidence tokens at issue in this Breach was the "FB4A" token, also known as the "Facebook For Android" token.[7] The FB4A token was specifically designed to persist (never expire) even if the user logged out of the application or opted out of the entire platform (i.e., removed Facebook from his/her device and closed his/her user account).[8]

In 2017, Facebook enhanced the risks of NoConfidence tokens when it reintroduced its "View As" feature. This permitted users to "view" their profiles as one of their friends.[9] To enable the "View As" function, Facebook used the FB4A token, even though Facebook's own software and security engineers expressed continued concern that the FB4A token gave substantially more permissions to information and platform access than the function needed.[10]

### B. Facebook Recognized But Disregarded the Risks it Created

Right up until the Breach, Facebook engineers were sounding the alarm about the huge security risks these tokens created. Whether due to organizational lassitude, limited manpower, or an unwillingness to upset revenue flows, Facebook disregarded the risks of the highly permissioned

[3] Ex. 2, Declaration of Mary Frantz ("Frantz Decl.") at ¶¶ 4, 6, 43. Ms. Frantz is the Founder and Managing Partner of Enterprise Knowledge Partners, LLC (EKP), and specializes in eDiscovery, Forensics, Cyber Security and Enterprise Architecture. She previously appeared before this Court for the January 9, 2019 tutorial.

[4] *Id.* at ¶¶ 17, 18, 20, 21, 27, 37, 41(A). 41(D)–(G), 43, 60, 61(A), 61(D), 61(E).

[5] *Id.* at ¶ 43.

[6] *Id.* at ¶¶ 18, 43.

[7] Facebook develops its code based upon the Android operating system, because Google made the mobile android operating system open source. *Id.* at ¶¶ 42, 58, 61(A), 61(E).

[8] *Id.* at ¶¶ 20, 41(D), 61(D).

[9] ECF No. 97, Declaration of Christopher Bream ("Bream Decl.") ¶ 13(a); *see also* Ex. 3, FB-SCHMIDT-000000487, at '491

[10] Ex. 2, Frantz Decl. at ¶¶ 20, 21, 41(A), 41(D)–(G), 61(A).

access tokens and did not change its authentication infrastructure. The limited documents reviewed to date show numerous times "tasks" were created that would address the permissiveness of the access tokens, but then abandoned. For example:

- *Facebook Messenger:* In March 2016, Facebook engineers opened a task called [redacted]"[11] This discussed a function associated with the use of an FB4A token that could [redacted].[13] The last entry on March 10, 2018 states is an automated message, "[redacted]."
- *Video Uploader:* Throughout 2017, [redacted].[14] By December 2017, Neal Poole, a software engineer at Facebook who was part of the Product Security Team, and who was heralded as one of the most talented engineers at Facebook by former Facebook CSO Alex Stamos,[15] concluded from these discussions that [redacted] writing [redacted][16] In other words, if these tokens became compromised, the attacker could access the user's profile without the user's knowledge.[17] Furthermore, an attacker with access to an already compromised account could potentially extract the FB4A token and use it

[11] Ex. 4, FB-SCHMIDT-000053846

[12] *Id.*

[13] *Id.*

[14] *See* Ex. 5, FB-SCHMIDT-000052617; Ex. 6, FB-SCHMIDT-000054527; Ex. 7, FB-SCHMIDT-000053863. There is no evidence that the Video Uploader code was ever security tested. Ex. 2, Frantz Decl. at ¶¶ 37, 38, 41(D)–(F).

[15] Ex. 8, August 22, 2019 Deposition of Alex Stamos at 314:1-4

[16] Ex. 9, FB-SCHMIDT-000054518 (emphasis added).

[17] Ex. 2, Frantz Decl. at ¶¶ 4, 5, 7, 20, 34, 43, 46, 59, 95, and 96.

to request additional information despite no longer having physical access to the device from which it was generated.[18] But Facebook proceeded with the Video Uploader.

- “[redacted]In early 2018, an internal task was created, [redacted][19] Facebook personnel became cognizant that the FB4A token did not expire or become invalid after a user logged out, unless the user knew to log out of *all* sessions.[20] Ben Yang wrote on July 18, 2018: “[[redacted].”[21] However, Steve Gao replied that “[redacted]hus interfering with Facebook’s ability to generate revenue. [22] While the “[redacted]” task was created on May 18, 2018, it repeatedly lay dormant with no activity, prompting automated messages.”[23] It was not completed. [24]
- [redacted]”: On July 10, 2018, Nishith Nand (another Facebook software engineer) created a task called, “[redacted][25] S[redacted][26] The risks she noted were that the impersonator could [redacted]]”[27] She noted multiple YouTube videos

[18] Ex. 10, July 3, 2019 Deposition of Neal Poole (“Poole Dep.”) at 82:18-25, 83:16-24; Ex. 2, Frantz Decl. at ¶¶ 4, 6, 17, 18, 20, 21, 27, 37, 41(A), 41(D)–(G), 43, 60, 61(A), 61(D), 61(E).

[19] Ex. 11, FB-SCHMIDT-000054260 (emphasis in original).

[20] *Id.* ([redacted] Later notes indicate that the only option is “[redacted]

[21] *Id.* at ‘261.

[22] *Id. See also* Ex. 2, Frantz Decl. at ¶¶ 23, 31, 27, 41(A)–(H), 76.

[23] *Id.* [redacted]

[24] *Id.* Later, one of the employees working on the task testified [redacted]. Ex. 12, July 25, 2019 Deposition of Kyle Minshall at 261:23 – 263:15, 265:24 – 266:17.

[25] Ex. 1, FB-SCHMIDT-000054545, at ‘548.

[26] *Id.* at ‘547.

[27] *Id.* at ‘545.

on how to harvest and exploit these tokens.[28] Nand listed actions and remedial measures she thought should happen soon, ([redacted]).”[29] Another engineer asked if she needed help as she too saw the risk:

> [redacted]
>
> [redacted]
>
> [redacted][30]

There was no action on this task for weeks, and it was marked closed out after the Breach.

In addition to tasks begun and forgotten, Facebook personnel like Neal Poole exchanged elaborate emails that discussed the risks of the access tokens. For example, on August 24, 2018, employee Dan Xu warned Neal Poole: “[redacted].”[31] Poole agreed: “[redacted].”[32] Poole later wrote, “[redacted]

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Ex. 13, FB-SCHMIDT-000064914 at ‘917.

[32] *Id.*

[redacted][33] He was to meet with others on the security team the week of September 17, 2018 to discuss this further. By then, the Breach was underway.[34]

Finally, there is the ignored Tweet. On September 5, 2018, a software engineer tweeted at Facebook (including CEO Mark Zuckerberg) that he saw a "glitch": that shows "JSON on iphone app when we see our profile in 'View As' mode, and then click profile pic, then click OK."[35] [redacted] on September 29, 2018,[36] after the breach.

### C. Facebook's Slow Response Allowed Thieves To Steal the PII of Millions

Compounding its self-created vulnerability to the hack was Facebook's response to the Breach. Facebook claims it first learned of a potential data breach on September 17, 2018, when it noticed "an unusual spike of activity" among users that had been inactive for at least 30 days.[37] But it was Facebook's ***Growth Team*** that "opened an investigation as part of its routine work validating user metrics."[38] As the name implies, the Growth Team is not primarily, or even secondarily, focused on security, but on increasing signups, activating as many users as possible, retaining users, and bringing churned users back into Facebook.[39] "[redacted]" but did not find an adequate explanation for a spike.[40] Several members of that team opened up "SEVs" or "site events", but did not determine what was causing the spikes.[41] Not until September 25, 2018, did the Growth Team call on the Security Team.[42]

[33] *Id.*

[34] *Id.* at '914. Facebook produced this document (and about 4,800 others) on August 16, 2019, more than a month after Mr. Poole's deposition and less than two weeks before the due date for the motion for class certification. Plaintiff was not able to examine him about this.

[35] Ex. 14, Sept. 5, 2018 tweet from Amit Baghel. (https://twitter.com/CodingKeeda/status/1037236528093835264).

[36] Ex. 15, FB-SCHMIDT-000052079.

[37] Ex. 3, at '491.

[38] *Id.*

[39] Quora, "How The Growth Team Helped Facebook Reach 500 Million Users," *Forbes*, Sept. 15, 2014, as seen at https://www.forbes.com/sites/quora/2014/09/15/how-the-growth-team-helped-facebook-reach-500-million-users/#785c61270580.

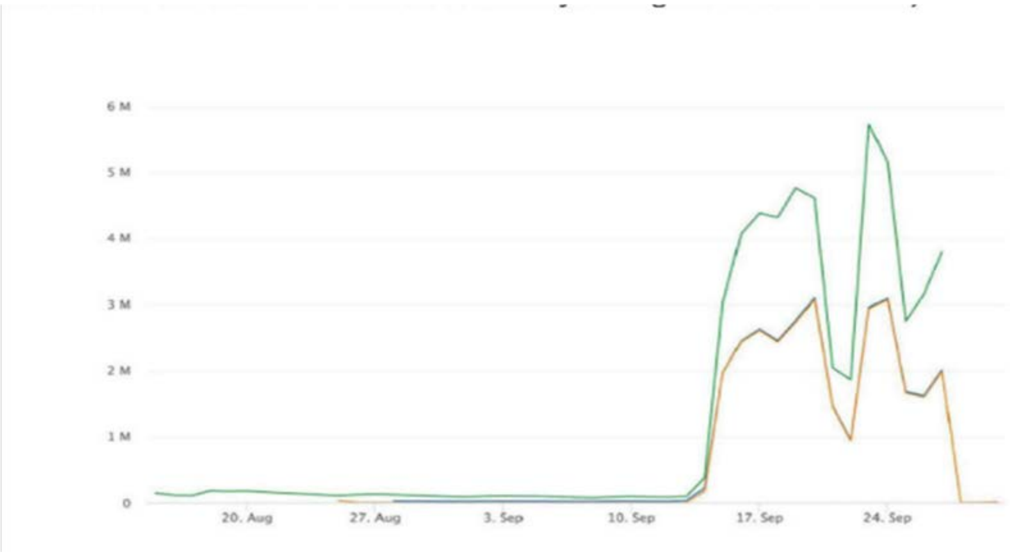
[40] Ex. 3 at '491.

[41] Ex. 16, FB-SCHMIDT-00000102 at '103. *See also* Ex. 17, April 12, 2019 Rule 30(b)(6) Deposition of Christopher Bream ("Bream 30(b)(6) Dep.") at 43:22-46:14.

[42] *Id.*

The Security Team found that the attack had begun on September 14, 2018.[43] The hackers used access tokens stolen for "seed" users during the attack, and then through a series of automated scripting, the hackers used the seed user's timeline posts to bring birthday events to the top of the timeline and get "happy birthday" messages. The hackers thereafter moved on to breaching the Friends of that users' accounts.[44]

The delay between the Growth Team's first noting the spike and the escalation to the Security team was costly. As depicted in the Facebook graph below, each day the Breach went on (see x axis), the attackers obtained access tokens and PII of millions of users (see y axis).[45]



The security team Facebook set up a war room, alerted senior management, and then started invalidating access tokens and logging off customers on September 27, 2018—10 days after the Growth Team saw the strange spike.[46]

### D. Facebook Admits its Negligence

After the Breach, many Facebook employees admitted their neglect internally, and discussed how Facebook could have avoided this fiasco. Joseph Adler noted, "[redacted]

[43] Ex. 3, at '489.

[44] *Id.*

[45] *Id.* [redacted] *Id.*

[46] *Id.* at '492.

[redacted][47] Another employee, Steve DeLucia lamented, "[redacted]."[48] Ben Yang noted, [redacted][49] Neal Poole, who [redacted]s weeks before the Breach,[50] responded with an acknowledgment of the admission and an old-school emoji: [redacted] [redacted] Yang replied, [redacted]."[52] Stephen Sclafani questioned why Facebook had not caught the vulnerability, noting [redacted][53]

On October 5, 2018, Facebook's Peng Tian sent a follow up report to a team working on authentication infrastructure, stating in no uncertain terms that "[redacted]"[54] Stunningly, Tian admitted, that "[redacted][55]

**E. Impact of the Breach**

In the end, Facebook allowed the attackers to gain access to over 300,000 Facebook accounts, and exploit those accounts to then steal 29 million Facebook users' access tokens. Bream Decl. at ¶¶ 11-12. Facebook categorized the affected users as:

[47] Ex. 18, FB-SCHMIDT-000053844.

[48] *Id.* at '845. *See also* Ex. 19, FB-SCHMIDT-000055983 (Nov. 2018 note from Kyle Minshall: [redacted]

[49] Ex. 20, FB-SCHMIDT-000052491, at '492 (emphasis added).

[50] Ex. 13, at '917.

[51] *Id.*

[52] *Id.*

[53] Ex. 21, FB-SCHMIDT-000049965 at '974.

[54] Ex. 22, FB-SCHMIDT-000055511 at '512 (emphasis added).

[55] *Id.* Scott Renfro, Pedro Canahuati (head of security), and Gregg Stefanik [redacted]

**Group 1**: For approximately 15 million users, including approximately 2.7 million users in the United States, the attackers obtained the user's name, email address and/or phone number;

**Group 2**: For approximately 14 million users, including approximately 1.2 million users in the United States, the attackers obtained the information above plus username, first name, last name, full name, gender and date of birth, and, to the extent the fields were populated, workplace, education, relationship status, religious views, hometown, self-reported current city, and website. Also obtained was the Facebook locale/language; the types of device(s) used by the user to access Facebook; the last 10 places the user "checked into" or was "tagged" in on Facebook, if any; the people or pages on Facebook followed by the user, if any; and the user's 15 most recent searches using the Facebook search bar, if any.

**Group 3:** For about 300,000 users, the attackers obtained the same data in Group 2, but also accessed additional profile data as part of its operation: they used these "seed" user's accounts to repeatedly load up their profiles to capture the underlying HTML where the Friend's access tokens were rendered.[56]

From these groups, certain historical PII was taken—this is PII that cannot be easily changed and is often used as the basis for identity theft or to circumvent challenge questions that the users may have for other online protocols.[57]

### E. Plaintiff's Claims and Motion for Class Certification

Plaintiff seeks class certification for two claims: negligence and declaratory judgment. Plaintiff seeks certification under Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the following class:

**All Facebook users whose PII was part of the September 2018 Data Breach.**

Plaintiff seeks class injunctive relief under Rule 23(b)(2)—namely a set of changes in Facebook's conduct to ensure no further harm. Plaintiff seeks class damages under Rule 23(b)(3), specifically damages related to the diminished value of their PII, and for Facebook to provide the

[56] Bream Decl. at ¶¶ 11-13. Facebook claims it was unlikely the attackers took additional information from the profile pages of Group 3. Ex. 23, FB-SCHMIDT-00000198 at '212. As such, Plaintiff treats Group 3 users the same as Group 2.

[57] Ex. 2, Frantz Decl. at ¶¶ 7, 27, 64, 81–103

money for credit monitoring. Finally, Plaintiff seeks certification of a class under Rule 23(c)(4) for those who seek additional individual damages resulting from the time spent devoted to the Breach or any losses for identity theft they can tie to the Breach.

## **LEGAL STANDARD**

To certify a class under Federal Rule of Civil Procedure 23, a plaintiff must demonstrate numerosity, commonality, typicality, and adequacy, and satisfaction of the requirements for one of the class types defined in Rule 23(b). *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 979–80 (9th Cir. 2011). To certify a Rule 23(b)(2) class, the plaintiff must show that "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Certification under Rule 23(b)(3) requires that "'questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.'" *Sali v. Corona Reg'l Med. Ctr.*, 889 F.3d 623, 629 (9th Cir. 2018). Rule 23(c)(4) provides the court with discretion to certify a class to resolve particular issues, such that "[e]ven if the common questions do not predominate over the individual questions," a court may "isolate the common issues . . . and proceed with class treatment of these particular issues." *Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1234 (9th Cir. 1996).

A "'rigorous analysis'" is required, *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 586 (N.D. Cal. 2015), but this does not require or warrant "a mini-trial." *Sali*, 889 F.3d at 631. Nor is the district court "limited to considering only admissible evidence in evaluating whether Rule 23's requirements are met." *Id.* at 632. Where the merits are probed, they may be so only to the extent "that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Amgen Inc. v. Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 466 (2013). Plaintiff meets his burden under Rule 23, such that certification of the proposed Classes is warranted.

## ARGUMENT

## I. THE PROPOSED CLASSES MEET RULE 23(a) REQUIREMENTS

### A. With 29 Million Users Breached, Numerosity is Met

Facebook concedes that 29 million user accounts have been compromised, including more than four million U.S. users. Bream Decl. at ¶ 11. Thus, the proposed classes are sufficiently numerous. *Rannis v. Recchia*, 380 F. App'x 646, 651 (9th Cir. 2010) (noting numerosity usually met with at least 40 class members).[58]

### B. Facebook's Conduct Related to The Breach Raises Common Legal and Factual Questions

Rule 23(a)(2) requires "questions of law or fact common to the class." A single common question is sufficient. *See Ellis*, 657 F.3d at 981. A common question is one that "generate[s] common answers apt to drive the resolution of the litigation." *Torres v. Mercer Canyons Inc.*, 835 F. 3d 1125, 1133 (9th Cir. 2016). The claims here easily meet this standard. Each Class member's PII was compromised due to an access token security vulnerability. Therefore, proof of what Facebook knew about its access tokens and what it did or did not do to address this vulnerability is common to all class members, regardless of whether they fall into Group 1, 2, or 3. The requisite commonality exists here because the issues raised by the classes' claims have common answers that will drive the resolution of this case. These include:

- Whether Facebook owed a duty to exercise due care in collecting, storing, and safeguarding PII;
- Whether Facebook breached that duty;
- Whether Facebook knew about the security risk posed by the persistent access tokens (and when);
- Whether Facebook's failure to remedy an obvious and known security risk posed by persistent access tokens was affirmative negligence;

[58] The proposed class members will be readily ascertainable from Facebook's records. Plaintiff does not address this any further in light of *Briseno v. Con Agra Foods, Inc.*, 844 F. 3d 1121, 1133 (9th Cir. 2017).

- Whether by permitting its Growth Team to dawdle while the breach was underway, Facebook committed affirmative negligence;
- Whether Facebook's negligence caused harm to Plaintiff and class members;
- Whether Facebook and its users have a special relationship in light of the information shared precluding application of the economic loss rule; and
- Whether Facebook's security is still inadequate to protect user PII.

### C. Plaintiff's Claims are Typical of the Class

Rule 23(a)(3)'s typicality standard is met when the class representative's claims arise from the same course of events and rely on similar legal arguments as other class members' claims. *Parsons v. Ryan*, 754 F.3d 657, 685 (9th Cir. 2014). These claims "need not be substantially identical." *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1020 (9th Cir. 1998). Plaintiff's PII was compromised in the same Breach as was the PII of other class members. Thus, typicality is necessarily satisfied where, as here, "the plaintiff endured a course of conduct directed against the class." *Just Film v. Buono*, 847 F.3d 1108, 1118 (9th Cir. 2017).

Plaintiff's claims and legal theories, both in his individual and representative capacities, arise under the same factual predicate. The elements Plaintiff must prove for negligence are identical to what absent class members would need to prove, and there are no defenses unique to Plaintiff. Plaintiff's affirmative negligence claim is also typical to the nationwide class because, like all class members, he was harmed by Facebook's access token vulnerability and its failure to remedy the vulnerability despite long-term knowledge of its existence. In other words, he was subject to the same decision-making as were other Class members. He, and class members, face the same risk of identity theft (negligence), and same need for future protection of their PII (declaratory judgment).

### D. Plaintiff and Counsel are Adequate

Rule 23(a)(4) requires the class representative to "fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). Adequacy is satisfied when 1) the named plaintiff and counsel have no conflicts with the class; and 2) plaintiff will "prosecute the action vigorously." *Staton v. Boeing Co.*, 327 F.3d 938, 957 (2003); *see also* Fed. R. Civ. P. 23(a)(4). Plaintiff has no conflicts with the class, and instead shares the same interests in prosecuting these claims. He has participated actively in this case, including by reviewing pleadings, responding to discovery, and sitting for a deposition.

Proposed class counsel, approved by this Court as interim lead counsel, are experienced class action attorneys and are committed to prosecuting this case. (ECF Nos. 72, 79). To date, class counsel have: 1) propounded and responded to discovery and engaged in discovery motion practice; 2) argued motions to dismiss and amend the pleadings; 3) reviewed and coded documents (this process is ongoing); 4) deposed eight current and former Facebook employees in San Francisco, Seattle, New York, and London, U.K.; 5) deposed three corporate representatives under Rule 30(b)(6); 4) engaged an cybersecurity expert to opine on Facebook's negligent security practices, and appropriate equitable relief to change those practices; and 6) engaged financial experts to provide models for class members' recovery. Thus, Plaintiff and proposed Class Counsel meet the adequacy requirement.

## II. THE COURT SHOULD CERTIFY A 23(b)(2) CLASS FOR DECLARATORY RELIEF

Class certification of a claim for declaratory relief is appropriate when, in addition to the four requirements of Rule 23(a) discussed above, "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief … is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). "Unlike Rule 23(b)(3), a plaintiff does not need to show predominance of common issues or superiority of class adjudication to certify a Rule 23(b)(2) class." *Yahoo Mail*, 308 F.R.D. at 587; *see also Brazil v. Dole Packaged Foods, LLC*, 2014 WL 2466559, at *10 (N.D. Cal. May 30, 2014) ("Ordinarily, it follows that there is no need [in evaluating a Rule 23(b)(2) class] to undertake a case-specific inquiry into whether class issues must predominate or whether class action is the superior method of adjudicating the dispute [.]'"). (internal citation omitted).

Here, Plaintiff's declaratory relief claim meets that standard because Facebook acted in a manner common to the Class. Facebook subjected all Class members' PII to the same security vulnerability (persistent access tokens too highly permissioned for the function assigned); Class members' PII was compromised as a result of that vulnerability; Facebook is still in possession of Class members' PII; and Facebook still has not adequately secured the PII. Injunctive relief is thus needed to remediate Facebook's inadequate security, which uniformly applies to all Class members. Plaintiff's expert Mary Frantz has set forth the security controls needed to protect class members' PII in the future. These include:

- Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Facebook' systems on a periodic basis
- Ordering Facebook to promptly correct any problems or issues detected by such third-party security auditors;
- Engaging third-party security auditors and internal personnel to run automated security monitoring; auditing, testing, and training its security personnel regarding any new or modified procedures;
- Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;
- Conducting regular database scanning and securing checks; and routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach
- Invalidating persistent access tokens and warning users to log off of all sessions on all devices periodically.

*See* Ex. 2, Frantz Decl. at ¶¶ 104, 105; *see also* FACC ¶ 221.

## III. RULE 23(b)(3) CERTIFICATION OF THE DAMAGES CLASS IS PROPER

There is "clear justification for handling the dispute on a representative . . . basis if common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication." *In re Lenovo Adware Litig.*, 2016 WL 6277245, at *17 (N.D. Cal. Oct. 27, 2016) (internal citations omitted). The common questions can be resolved in one fell swoop, as demonstrated below.

### A. Common Questions of Law and Fact Predominate

"The predominance analysis under Rule 23(b)(3) focuses on the relationship between the common and individual issues in the case, and 'tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *Just Film*, 847 F.3d at 1120 (internal citations omitted). It generally begins with an examination of the elements underlying a plaintiff's causes of action. *Ellsworth v. U.S. Bank, N.A.*, 2014 WL 2734953, at *19 (N.D. Cal. June 13, 2014). "In determining whether common questions predominate, the Court identifies the substantive issues related to plaintiff's claims (both the causes of action and affirmative defenses); then considers the proof necessary to establish each element of the claim or defense; and considers how these issues would be tried." *Id.* Where, as here, the conduct giving rise to both the duty and breach is uniform, Plaintiff's negligence claim is appropriate for classwide resolution as questions of legal duty and Facebook's breach of that duty are common issues susceptible to common proof. *See Giroux v. Essex Prop. Tr., Inc.*, 2018 WL 2463107, at *4 (N.D. Cal. June 1, 2018); *see, e.g.*, *Smith v. Triad of Alabama, LLC*, 2017 WL 1044692, at *13 (M.D. Ala. Mar. 17, 2017) (certifying negligence class in data breach suit against hospital where each class member was a "non-hospital" patient at the hospital, alleged injury as a result of a rogue employee's theft of records, suffered the same general type of damages, and class members' claims were subject to a single state's law), *aff'd on reconsideration*, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017).

Plaintiff (and class members) must prove the same elements to prevail on their negligence claim: (1) a duty; (2) breach of that duty; (3) causation; and (4) a cognizable injury. *Ileto v. Glock Inc.*, 349 F.3d 1191, 1203 (9th Cir. 2003) (citing *Martinez v. Pacific Bell*, 225 Cal. App. 3d 1557, 275 (1990)).[59] The common evidence supports these elements.

### 1. Facebook Has a Duty to Protect Users' PII

Plaintiff, like each class member was a Facebook user, and each entrusted Facebook with some PII in exchange for Facebook's service. FACC ¶¶ 11, 21, 22, 25. Since Facebook accepted this data, it was obligated to protect it. *See, e.g.*, *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) (to hold that no duty to safeguard consumer PII exists "would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyberattacks leaving consumers with no recourse to recover damages

[59] In addition, classwide application of California law moots many of the predominance concerns nationwide negligence classes often raise. *See Marsh v. First Bank of Del.*, 2014 WL 554553, at *16 (N.D. Cal. Feb. 7, 2014) (certifying negligence class under California law).

even though the retailer was in a superior position to safeguard the public from such a risk.”).

Plaintiff can show the existence of this duty on a classwide basis. Facebook understood that the access tokens were the functional equivalent of passwords: “[redacted].[60] This Court has already determined that an access token is a “password.” (ECF No. 153 at 3). As such, Facebook was obligated to protect user’s access token under the California Customer Records Act (Cal. Civ. Code §§ 1798.80, *et seq*.), which requires businesses to ensure that personal information about California residents is protected. Facebook admits that at minimum 70,000 users had their access tokens compromised in the Data Breach.[61] At least some of these users are California residents.[62]

Facebook’s duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45(a), which prohibits “unfair . . . practices in or affecting commerce,” including, as enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Facebook. Various FTC publications and data security breach orders further form the basis of Facebook’s duty.[63] Facebook’s employees understood this duty:

> [redacted][64]

Mark Zuckerberg himself proclaimed it, “We have a responsibility to protect your data, and

[60] Ex. 1, FB-SCHMIDT-000054545.
[61] Ex. 24, May 2, 2019 Hearing Tr. at 51:19-23.
[62] *Cf. id.* at 12:22 (Defendant contends only that “most of the class are not California residents[.]”)
[63] *See, e.g., Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 30, 2019), *available at*: https://www.gao.gov/products/GAO-18-559 (regarding the Equifax data breach).
[64] Ex. 25, August 8, 2019 Deposition of Brad Hill at 41:10-42:1 (objections omitted).

if we can’t then we don’t deserve to serve you.”[65]

### 2. Facebook Breached its Duty

Common evidence shows that Facebook failed to adequately safeguard users’ PII and continues to do so. Specifically, Facebook used persistent access tokens, such as the FB4A token, even though its personnel knew that the tokens were a security risk. *See* Ex. 4 (discussing FB4A tokens with messenger) and Exs. 5-7 (related to View As); and Ex. 13 at ‘917 (related to Community Risk assessment). Facebook received warnings from at least one of its users, Ex. 14 (Sept. 5, 2018 tweet), and opened (but never finished) tasks to address the risk of persistent tokens, Exs. 1 & 11. This led to a sea of admissions post-Breach. *See, e.g.*, Ex. 18 (“[redacted]); Ex. 20 at ‘492 (“[redacted] *See also* Exs. 19, 21 & 22.

Common evidence also shows that Facebook failed miserably in its initial response to the Breach. [redacted]. Ex. 3 at ‘491. [redacted] *Id.* According to Bream [redacted].” Ex. 17, Bream 30(b)(6) Dep. 40:23–41:10, 43:22–45:19. When it did notify [redacted] *Id.* Not until September 25, 2018 did the Growth Team [redacted] *Id.* By then, millions of users had their PII scraped. Ex. 3, at ‘491. Thus, this inept response to the Breach can be shown with common evidence.

### 3. Common Evidence Supports Causation

Plaintiff may establish classwide causation under California’s “substantial factor” test. *See*

[65] Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018), *available at*: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

*Mitchell v. Gonzales*, 54 Cal. 3d 1041, 1044 n.2, 1052 (1991) (negligence); *In re San Jose Airport Hotel, LLC*, 2018 WL 1426702, at *5 (N.D. Cal. Mar. 22, 2018) (contract). "The substantial factor standard . . . has been embraced as a clearer rule of causation – one which subsumes the 'but for' test while reaching beyond it to satisfactorily address other situations, such as those involving independent or concurrent causes in fact." *Rutherford v. Owens-Illinois, Inc.*, 16 Cal. 4th 953, 968-69 (1997). Under this standard, a cause in fact is something that is a substantial factor in bringing about the injury. *Mitchell*, 54 Cal. 3d at 1052-53; *see also Britz Fertilizers, Inc. v. Bayer Corp.*, 665 F. Supp. 2d 1142, 1172 (E.D. Cal. 2009).

Here, Plaintiff can show that the Breach caused millions to lose their PII through common evidence, including Facebook's concessions. Bream Decl. at ¶ 11. Further, through expert testimony, Plaintiff can show that he and all class members face increased risks of identity theft. *See* Ex. 26, Declaration of Ian Ratner ("Ratner Decl.") at ¶ 39; Ex. 27, Declaration of Jim Van Dyke ("Van Dyke Decl.") at 11-15. Finally, common evidence can also show the Breach caused a decline in the value of their PII (given that it was now available on the Dark Web). Ex. 26, Ratner Decl. at ¶¶ 45-46.

### 4. Damages as to PII and Credit Monitoring Can be Established Classwide

Facebook's negligence caused each class member a cognizable injury: lost value of PII; time spent addressing the consequences of the Breach; and the cost of ongoing credit monitoring. FACC ¶ 212. Each has the "real anxiety and harm to the individual person who has to go the rest of their life worrying whether or not this Facebook breach is going to come back to haunt them in ten years, or five years, or three years." Ex. 28, Jan. 9, 2019 Tutorial Proceeding Tr. at 108:16-19.

That some or all of the damages may ultimately require individual calculation, does not defeat class certification. *Pulaski & Middleman, LLC v. Google, Inc.*, 802 F.3d 979, 988 (9th Cir. 2015), cert. denied, 136 S. Ct. 2410 (2016) ("differences in damage calculations do not defeat class certification"); *see also Just Film*, 847 F.3d at 1120–21 (certifying class when one method of calculating damages was based on class members using their individual records to show their expenses, including time and effort expended); *Nitsch v. Dreamworks Animation SKG Inc.*, 315

F.R.D. 270, 313 (N.D. Cal. 2016) (certifying class where "defenses peculiar to some individual class members will have to be tried separately").

Here, two damages may be established classwide: the diminished value of PII, and the costs of credit monitoring. First, Plaintiff Adkins and the users affected by the Breach provided valuable PII to Facebook, which it then monetized. Facebook has identified the PII taken. Ex. 23 at '210-212. This PII can be ascribed value through many ways, including looking at its value on the Dark Web. Ex. 26, Ratner Decl. at ¶ 50. Plaintiff's expert, economist Ratner, has estimated the value of the PII taken at $15,000,000 to $35,254,667 for Group 1 users, and $56,000,000 to $87,234,012 for Group 2. *Id.* at ¶¶ 54-59.

The Data Breach was a substantial factor in causing Plaintiff's need for ongoing and future credit monitoring services. Jim Van Dyke, Founder and CEO of Futurion.digital, Inc., specializes in consumer identity fraud and security. Ex. 27, Van Dyke Decl. at 1. He will testify of the risks to PII being stolen, *Id*. at 4-9, particularly the PII at issue in the Breach, *Id*. at 11-15. He also has classwide recommendations to mitigate the risks, including credit monitoring utilizing all three credit bureaus, for at least five years. *Id*. at 23. Mr. Ratner has priced out plans that include such coverage and insurance and estimates the costs for such credit monitoring at between $1,045 (using a subscription rate of $219) and $1,574 (using a subscription rate of $330). Ex. 26, Ratner Decl. at ¶¶ 40-44.

Common evidence shows that credit monitoring is warranted here. First, the significance and extent of the compromise to Plaintiffs' PII includes historical PII.[66] This information is a building block for identity theft and can be used to circumvent challenge questions.[67] The risks of identity theft to Adkins and class members increased in light of the theft when compared to their chances of identity theft had the data breach not occurred, especially considering the aggregated nature of Plaintiff's and class members' PII on Facebook.[68] The severity of the consequences

[66] Ex. 2, Frantz Decl. at ¶¶ 7, 27, 64, 81–103.

[67] Ex. 2, Frantz Decl. at ¶¶ 7, 27, 64, 81–103.

[68] Ex. 2, Frantz Decl. at ¶¶ 7, 27, 64, 81–103.

resulting from identity theft are not disputed; nor could they be when Facebook itself recognized the need to log out 90 million users to protect them against further risk that the hackers would get their access tokens. Ex. 3 at ‘492. Finally, early detection can help class members avoid the consequences of identity theft. *Corona v. Sony Pictures Entertainment, Inc.*, 2015 WL 3916744 at* 4 (C.D. Cal. June 15, 2015) (recognizing credit monitoring where among the sensitive data stolen was "names, home and email addresses," and that the "risk of identity theft" was "both serious and long-lasting", making early detection valuable.). Plaintiff Adkins considered the purchase of credit monitoring but found it too costly given his economic means. Ex. 29, May 9, 2019 Deposition of Stephen Adkins ("Adkins Dep.") at 267:10–268:13.

Finally, the Court can also decide Plaintiff's request for punitive damages on a classwide basis. *Opperman v. Path, Inc.*, 2016 WL 3844326, at *16 (N.D. Cal. July 15, 2016) ("Because the purpose of punitive damages is not to compensate the victim, but to punish and deter the defendant, any claim for such damages hinges, not on facts unique to each class member, but on the defendant's conduct toward the class as a whole."). Here, Facebook's affirmative negligence—which included deliberate disregard for a known risk—can be shown based upon the common evidence discussed herein.

#### 5. The Economic Loss Rule Is a Predominating Legal Question Plaintiff Can Defeat with Common Evidence

A final matter that can be addressed by common evidence is Facebook's likely assertion of defense based upon the economic loss rule. Def. Mot. to Dismiss (ECF No. 96) at 23. In addition to clearly being a common question, it is inapplicable here. Facebook has a "special relationship" with its users, which precludes application of the economic loss rule. *J'Aire Corp. v. Gregory*, 24 Cal.3d 799, 804 (1979); *see* FACC ¶ 204. California courts may find a special relationship when there is an agreement for services between the parties. *N. Am. Chem. Co. v. Sup. Ct.*, 59 Cal. App. 4th 764 (1997). Courts in this District have already found that Facebook provides a service. *See, e.g., In re Facebook Privacy Litig.*, 192 F. Supp. 3d 1053, 1055 (N.D. Cal. 2016) ("Facebook provides social networking services…"). Where services are involved, courts ascertain a special relationship by looking at: (1) the extent to which the transaction was intended to affect the plaintiff;

(2) the foreseeability of harm to the plaintiff; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm. *In re Yahoo! Inc. Customer Data Sec. Litig.*, 313 F. Supp. 3d 1113, 1131 (N.D. Cal. 2018) (quoting *J'Aire, supra*). In a similar data breach case, Judge Koh found that Yahoo, a provider of a free internet service that accepted users' PII, entered into a special relationship with users so that the economic loss rule did not bar a negligence claim related to a data breach. *Id*. at 1132. First, just as in *Yahoo!*, the transaction entered into here was intended to affect the Plaintiff and the class in that it related to social media services for consumers. Second, it was foreseeable that Plaintiff would suffer injury if Facebook failed to adequately protect PII. Third, the hackers gained access to the PII, thereby causing injury to Plaintiff. Fourth, the injury was the direct result of Facebook providing inadequate security. Fifth, Facebook knew its lax data security history and that it was a target of hackers, but still integrated the Vulnerability. And sixth, Facebook's failure to adequately protect Plaintiff's PII implicates the consumer data protection concerns expressed in California and federal statutes. FACC ¶¶ 202-203; *Yahoo!*, 313 F. Supp. 3d. at 1132–33. In any event, the economic loss rule defense is completely appropriate for class-wide determination.

### B. A Class Action is Superior to Millions of Expensive Trials

Certification of Plaintiff's negligence claims would be "superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). Indeed, this is the kind of case for which the class action procedure was created. First, any Class member's individual recovery, even in cases of actual identity fraud, would be dwarfed by the cost of proving the predominating issues in this litigation. *Soares v. Flowers Foods, Inc.*, 320 F.R.D. 464, 485 (N.D. Cal. 2017) (Rule 23(b)(3)(A) "only weighs against class certification where individual damages 'run high' such that individual class members have a strong interest 'in making individual decisions on whether and when to settle'") (quoting *Amchem Prods. v. Windsor*, 521 U.S. 591, 616-17 (1997)). Second, no separate cases remain outside this proceeding indicating low or no interests to pursue the matter on an individual basis. *See* Fed R. Civ. P. 23(b)(3)(B). Third, Facebook's Terms of Service dictate all litigation must be brought under in this forum or in California. *See* Fed. R. Civ. P. 23(b)(3)(C). Finally, the issues presented in this class litigation are manageable in light of known users and one state law. *See* Fed. R. Civ. P. 23(b)(3)(D). A class action provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Individualized litigation would create a potential for inconsistent or contradictory judgments on the issues Plaintiff seeks to certify here (including, most notably, whether Facebook took adequate measures to protect users' PII) and would increase the delay and expense to all parties and the court system.

Notice should not be cumbersome. Each class member can be contacted directly by email and Facebook Messenger using Facebook's records. *See* Fed. R. Civ. P. 23(c)(2)(b). Otherwise, they may use publication through a variety of means for class members who no longer have their Facebook accounts. Further, because the Breach has been highly publicized around the world, a public notice in the U.S. would be effective.

Last, because class members can easily be verified using data maintained by Facebook—which has already identified compromised user accounts and notified the class members who own them—the claims process will be straightforward. *Id.* Thus, while ascertainability is not a requirement in the Ninth Circuit, *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1133 (9th Cir. 2017), the manageability problems that sometimes plague certification do not exist here.

## IV. THE COURT MAY ALSO CERTIFY COMMON ISSUES UNDER RULE 23(C)(4)

There are some damage claims that are not presently amenable to classwide disposition. For example, Plaintiff Adkins spent unreimbursed time logging back into Facebook, and canceling a credit card he worried might be affected. Ex. 29, Adkins Dep. at 66:7–14, 71:1–3, 194:12–19, 423:7–17. He also dealt with emails that he thought were "phishing scams." *Id.* at 198:10–13, 204:15–22. Plaintiff will use the testimony of Ian Ratner to show the value of that time on the labor market. Ex. 26, Ratner Decl. at ¶¶ 33-35. Mr. Ratner provides a formula to calculate the time spent (and value lost) dealing with the Breach: the total number of hours spent addressing the breach times the hourly rate for the value of hiring a bookkeeper/accountant/administrative assistant to deal with those matters. *Id*. at ¶ 36. Adkins can seek those damages individually, as could other class members. Additionally, those who believe they can show the Breach led to identity theft can use the class verdict on liability to pursue those additional consequential damages. Ex. 26, Ratner Decl. at ¶ 37. Plaintiff therefore, proposes the Court also certify a class under Rule 23(c)(4).

"When appropriate," Rule 23(c)(4) allows a court great discretion to certify an action "as a class action with respect to particular issues." Fed. R. Civ. P. 23(c)(4). It does not prescribe elements that representatives must show in order to maintain an issue class, but courts recognize its value in resolving cases where, though common questions may not predominate, denying certification of common issues would all but strip class members of their right to seek relief.

The Ninth Circuit has endorsed the use of issue certification. *Valentino*, 97 F.3d at 1234. So have many other circuit courts. *See In re Deepwater Horizon*, 739 F.3d 790, 817 (5th Cir. 2014); *Butler v. Sears, Roebuck & Co.*, 727 F.3d 796, 800 (7th Cir. 2013); *In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.*, 722 F.3d 838, 860 (6th Cir. 2013); *see also Jimenez II*, 765 F.3d at 1168 (noting *Butler, Whirlpool, and Deepwater Horizon* "are compelling . . .[a]nd their reasoning is consistent with our circuit precedent"). As explained above, basic liability questions predominate for Plaintiff's negligence claims. *Tasion Commc'ns, Inc. v. Ubiquiti Networks, Inc.*, 308 F.R.D. 630, 633 (N.D. Cal. 2015). The Court may certify issues under Rule 23(c)(4) if it materially advances the litigation as a whole, with the focus being "judicial economy and efficiency." *Kamakahi v. Am. Soc'y for Reprod. Med.*, 305 F.R.D. 164, 193 (N.D. Cal. 2015) (internal citations omitted). Importantly, the analysis focuses only on the issues to be certified. *See Deane v. Fastenal Co.*, 2012 WL 12552238, at *7 (N.D. Cal. Sept. 26, 2012).

A common trial on liability of Facebook for the Breach would materially advance the litigation. *Loritz v. Exide Techs., Inc*., 2015 WL 6790247, at *24 (C.D. Cal. July 21, 2015). Further, "Courts retain discretion to shape the proceedings and could ultimately choose an option such as the use of individual claim forms or the appointment of a special master, which plainly would allow [d]efendants to raise any defenses they may have to individual claims." *Jimenez v. Allstate Ins. Co.*, 765 F.3d 1161, 1168-69 (9th Cir. 2014) ("*Jimenez II*") (finding "statistical analysis [was] capable of leading to a fair determination of [defendant's] liability" and individualized damages hearings "preserved the rights of [defendant] to present its damages defenses on an individual basis"). The issues for trial would solely relate to Facebook's conduct; with individual follow-on proceedings for those seeking individual damages. If the answer to one or more of the questions is "No," then the litigation ends. If the answers are "Yes," then all remaining issues are capable of adjudication through a streamlined process that is far superior to requiring users to independently establish what Facebook did (or did not) do to safeguard PII and what Facebook knew and when. Thus, the answers would help to efficiently resolve the litigation.

## CONCLUSION

For the reasons stated above, Plaintiff's Motion for Class Certification should be granted.

DATED: August 29, 2019

Respectfully submitted,

By: /s/ Andrew N. Friedman
Andrew N. Friedman (*pro hac vice*)
**COHEN MILSTEIN SELLERS & TOLL PLLC**
1100 New York Ave. NW, Fifth Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699
afriedman@cohenmilstein.com

John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
**MORGAN & MORGAN**
**COMPLEX LITIGATION GROUP**
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: 813/223-5505
Facsmile: 813/2223-5402

Ariana J. Tadler (*pro hac vice*)
atadler@tadlerlaw.com
**TADLER LAW, LLP**
One Penn Plaza
New York, NY 10119
Telephone: (212) 946-9453

Facsimile: (212) 273-4375

*Interim Co-Lead Counsel for Plaintiff*

**CAPSTONE LAW, APC**
Tarek H. Zohdy (SBN 247775)
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett (SBN 275553)
Cody.Padgett@capstonelawyers.com
Trisha K. Monesi (SBN 303512)
Trisha.Monesi@capstonelawyers.com
Capstone Law APC
1875 Century Park East, Suite 1000
Los Angeles, California 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

**CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP**
David S. Casey, Jr. (SBN 060768)
dcasey@cglaw.com
Gayle M. Blatt (SBN 122048)
gmb@cglaw.com
Jeremy Robinson (SBN 188325)
jrobinson@cglaw.com
110 Laurel Street
San Diego, California 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232 fax

**CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION**
Clayeo C. Arnold (SBN 65070)
carnold@justice4you.com
Joshua H. Watson (SBN 238058)
jwatson@justice4you.com
865 Howe Avenue
Sacramento, California 95825
Telephone: 916-777-7777
Facsimile: 916-924-1829

**COHEN MILSTEIN SELLERS & TOLL PLLC**
Douglas J. McNamara
dmcnamara@cohenmilstein.com
Karina G. Puttieva (SBN 317702)
kputtieva@cohenmilstein.com
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

**FINKELSTEIN, BLANKENSHIP, FREI-PEARSON & GARBER LLP**
Jeremiah Frei-Pearson
Jfrei-pearson@fbfglaw.com
Andrew C. White
awhite@fbfglaw.com
445 Hamilton Ave., Suite 605
White Plains, New York 10601
Telephone: (914) 298-3281
Facsimile: (914) 908-6709

**FRANKLIN D. AZAR & ASSOCIATES**
Ivy Ngo (SBN 249860)
ngoi@fdazar.com
Kelly Hyman
hymank@fdazar.com
14426 East Evans Ave
Aurora, CO 80014
Telephone: 303-757-3300
Facsimile: 720-213-5131

**GLANCY PRONGAY & MURRAY LLP**
Marc Godino
mgodino@glancylaw.com
Brian Murray
bmurray@glancylaw.com
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: 310-201-9150
Facsimile: 310-432-1495

**JONES WARD PLC**
Jasper D. Ward
jasper@jonesward.com
1205 E Washington St, Suite 111
Louisville, Kentucky 40206
Telephone: 502-882-6000

**KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.**
Gary S. Graifman
ggraifman@kgglaw.com
Jay Brody
jbrody@kgglaw.com
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
Telephone: (845) 356-2570
Facsimile: (845) 356-4335

**KOHN, SWIFT & GRAF, P.C.**
Jonathan Shub (SBN 237708)
jshub@kohnswift.com
Kevin Laukaitis
klaukaitis@kohnswift.com
1600 Market Street, Suite 2500
Philadelphia, PA 19103-7225
Telephone: (215) 238-1700
Facsimile: (215) 238-1968

**LAW OFFICE OF PAUL C. WHALEN, P.C.**
Paul C. Whalen
paul@paulwhelan.com
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
Facsimile: (212) 658-9685

**LAW OFFICES OF CHARLES REICHMANN**
Charles Reichmann
Cpreichmann@yahoo.com
16 Yale Circle
Kensington, CA 94708
Telephone: (415) 373-8849

**LOCKRIDGE GRINDAL NAUEN PLLP**
Karen Hanson Riebel
khriebel@locklaw.com
Kate M. Baxter-Kauf
kmbaxter-kauf@locklaw.com
Arielle S. Wagner
aswagner@locklaw.com
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 596-4097
Facsimile: (612) 339-0981

**MIGLIACCIO & RATHOD LLP**
Nicholas A. Migliaccio
nmigliaccio@classlawdc.com
Jason S. Rathod
jrathos@classlawdc.com
412 H Street N.E., Ste. 302
Washington, DC 20002
Telephone: (202) 470-3520

**TADLER LAW LLP**
Ariana J. Tadler (*pro hac vice*)
ATadler@Tadlerlaw.com
One Penn Plaza
New York, New York
New York, NY 10119
Telephone: (212) 946-9453
Facsimile: (212) 273-4375

**MORGAN & MORGAN COMPLEX LITIGATION GROUP**
Ryan J. McGee
rmcgee@ForThePeople.com
Jean S. Martin
jeanmartin@ForThePeople.com
Kenya J. Reddy
kreddy@forthepeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

**ROBINSON CALCAGNIE, INC.**
Daniel S. Robinson (SBN 244245)
drobinson@robinsonfirm.com
Wesley K. Polischuk (SBM 254121)
wpolischuk@robinsonfirm.com
Michael W. Olson (312857)
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288

Facsimile: (949) 720-1292

**STULL, STULL & BRODY**
Patrice L. Bishop (SBN 182256)
pbishop@ssbla.com
Melissa R. Emert
memert@ssbny.com
9430 W. Olympic Blvd., Suite 400
Beverly Hills, CA 90212
Telephone: (310) 209-2468
Facsimile: (310) 209-2087

*Other Plaintiff's Counsel*