IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

ORDER ON MOTION FOR CLASS CERTIFICATION AND MOTIONS TO STRIKE

INTRODUCTION

This is a putative class action by plaintiff Stephen Adkins against defendant Facebook, Inc. Plaintiff asserts a claim for negligence based on Facebook's alleged faulty security practices in collecting and storing plaintiff's information. These faulty practices allegedly allowed hackers to break into Facebook's platform and pilfer the personal information of 29 million Facebook users worldwide, including more than four million users in the United States. The operative complaint seeks relief in the form of a credit monitoring service for the victims, in addition to compensatory, statutory, and punitive damages. The operative complaint also seeks declaratory relief (Amd. Compl. at 48) (Dkt. No. 193).

A prior order walked through the coding vulnerability which allowed the data breach (Dkt. No. 153). In brief, when three features on Facebook's platform interacted, "access tokens" became visible. Similar to a password, access tokens permitted users to enter their account. Once these access tokens became visible, those accounts became vulnerable to entry by strangers. In this way, the hackers entered 300,000 accounts in September 2018 (Bream Decl. ¶¶ 11–17; Amd. Compl. ¶¶ 95–97, 100) (Dkt. Nos. 97; 193)

The hackers ran two separate search queries from within these 300,000 accounts. The first yielded the names and telephone numbers and/or e-mail addresses of fifteen million users worldwide (2.7 million in the United States). The second yielded more sensitive information on fourteen million users worldwide (1.2 million in the United States). The information taken from this second group included names, telephone numbers, e-mail addresses, gender, date of birth, and, to the extent the fields were populated, workplace, education, relationship status, religious views, hometown, self-reported current city, and website. Within this second group, the hackers also obtained the user's locale and language, the type of device used by the user to access Facebook, the last ten places the user was "tagged" in or "checked into" on Facebook, the people or pages on Facebook followed by the user, and the user's fifteen most recent searches using the Facebook search bar. The original 300,000 users who had their accounts entered into also had the same information taken as this second group (Bream Decl. ¶¶ 10–12, 18–19).

In February 2019, five named plaintiffs filed a consolidated complaint which averred ten claims. An order consolidated eleven putative class action lawsuits filed in this district which arose from this data breach. Following Rule 12 practice, in August 2019, only one named plaintiff, Stephen Adkins, and two claims remained (Dkt. Nos. 76, 78, 96, 108, 113, 115, 153).

Plaintiff now seeks to certify a class of all Facebook users whose personal information became part of the September 2018 data breach. Plaintiff seeks certification under Rule 23(b)(2), Rule 23(b)(3), and Rule 23(c)(4). More specifically, plaintiff seeks injunctive relief for a *worldwide* class under Rule 23(b)(2), namely plaintiff seeks certain changes to Facebook's security practices to ensure no further harm comes to its users. Plaintiff seeks damages on behalf of a *nationwide* class under Rule 23(b)(3), related to the diminished value of personal information and for Facebook to provide cash for future credit monitoring. Finally, plaintiff seeks certification of a *nationwide* class under Rule 23(c)(4) for those who seek additional individual damages resulting from the time spent devoted to the data breach, and who incurred other individual injuries (Dkt. Nos. 193 at 47, 48; 198 at 1).

In opposing the class certification motion, Facebook concentrates most of its fire on the Rule 23(b)(3) damages class. Primarily, Facebook opposes on the ground that individual issues would predominate. Facebook also moved to strike two of plaintiff's expert declarations (Dkt. Nos. 213–15). This order follows oral argument.

ANALYSIS

This order first holds that plaintiff Stephen Adkins has sufficiently established Article III standing because of a substantial risk of identity theft and also because he has lost time due to the breach. Next, this order holds that Identity Theft Expert James Van Dyke's expert opinion must be excluded because his methodology is unreliable. CPA Ian Ratner's expert opinion, however, will be allowed. Finally, this order will certify an injunctive class under Rule 23(b)(2). The details now follow.

1. ARTICLE III STANDING.

A prior order dated June 21, 2019, held that plaintiff Adkins had sufficiently established standing (Dkt. No. 153 at 12). Then, as now, the only contentious element concerned the injury-in-fact requirement. Then, as now, plaintiff Adkins sufficiently established injury due to a substantial risk of future identity theft and also due to a continuing loss of time, all to follow.

A. Substantial Risk of Identity Theft.

No social security or credit-card numbers were taken in this hack. The hackers took plaintiff's name, date of birth, phone number, gender, and hometown, among other information (Dkt. No. 193 ¶ 102). Plaintiff, however, cannot change his date of birth or hometown and would not be expected to change his gender merely on account of a data breach. This information will abide, sensitive, long-term. This sensitivity, combined with the fact that the information was not merely taken, but specifically targeted for theft, continues to confer a basis for standing at this stage.

United States District Court
For the Northern District of California

Facebook complains that plaintiff has so far suffered only three [redacted] all of which went directly to his [redacted] But his identity remains at peril, theft-wise. That is enough.

A finding of a substantial risk of identity theft does not depend on concrete examples that the stolen information has already been misused. In *Krottner v. Starbucks Corporation*, "Starbucks sent a letter to . . . affected employees alerting them to the theft and stating that Starbucks had no indication that the private information ha[d] been misused." 628 F.3d 1139, 1140–41 (9th Cir. 2010) (internal quotation marks and citation omitted). Nevertheless, a credible threat of real and immediate harm had been sufficiently alleged there because the information: (i) had been sensitive and (ii) had been stolen. *Id*. at 1143. Plaintiff's risk of identity theft stems from the sensitivity of the information taken combined with its theft.

The information taken in *Krottner* — name, address, social security number — included information sufficiently similar to the information taken here. A social security number, though even worse to lose, is like one's date of birth, prior history, and gender. They remain with the victim forever, thereby "g[i]v[ing] hackers the means to commit fraud or identity theft." *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027–29 (9th Cir. 2018), *cert. denied sub nom., Zappos.com v. Stevens*, 139 S. Ct. 1373 (2019). Information such as this will never go bad, and so, hackers can warehouse this stolen data for years before using it. The substantial risk remains.

It is true that in *Zappos*, our court of appeals mentioned there were concrete examples of identity theft and specific instances of hacked accounts in that data breach, whereas in this case there are none. 888 F.3d at 1027–28. But *Zappos* also recognized that "[a] person whose [personal information] has been obtained and compromised may not see the full extent of identity theft or identity fraud for years. And it may take some time for the victim to become aware of the theft." *Id*. at 1028–29 (internal quotations omitted). Nothing in *Zappos* suggests that the absence of evidence of misuse kills standing. At this stage, information loss can be deemed sensitive without the victim being yet drained of identity.

According to Facebook, a social security number on its own can cause identity theft, whereas the information taken in this data breach does not have that power. Yet, one of

United States District Court
For the Northern District of California

[redacted] Even Facebook's own expert recognized outside this litigation that "investigators find that a cellphone number is often even more useful than a [s]ocial [s]ecurity number because it is tied to so many databases and is connected to a device you almost always have with you" (Dkt. No. 231-2 at 2). The *risk* of identity theft is imminent, without a multi-link chain of inferences, even though no social security number was taken.

The injury-in-fact requirement "helps to ensure that the plaintiff has a personal stake in the outcome of the controversy." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks and citation omitted). The information taken in this breach persuasively assures that plaintiff has such a stake. Plaintiff has established harm for Article III standing.

B. Loss of Time.

In the alternative, the prior order dated June 21, 2019, found that plaintiff Adkins had established Article III standing due to the harm of his loss of time. Plaintiff's expert now calculates that plaintiff spent [redacted] responding to this breach [redacted] Specifically, plaintiff Adkins testified he spent roughly [redacted] Plaintiff's expert calculates the total opportunity-cost of these damages as between [redacted]

At first blush, this amount of time might appear too small. A small injury, however, can still establish standing. As noted in the context of administrative standing by the United States Supreme Court in *United States v. Students Challenging Regulatory Agency Procedures (SCRAP)*, 412 U.S. 669, 689 n.14 (1973) (*citing,* Kenneth C. Davis, *Standing: Taxpayers and Others*, 35 U. Chi. L. Rev. 601, 613 (1968)):

> "Injury in fact" reflects the statutory requirement that a person be "adversely affected" or "aggrieved," and it serves

United States District Court
For the Northern District of California

> to distinguish a person with a direct stake in the outcome of a litigation — even though small — from a person with a mere interest in the problem. We have allowed important interests to be vindicated by plaintiffs with no more at stake in the outcome of an action than a fraction of a vote, see *Baker v. Carr*, 369 U.S. 186; a $5 fine and costs, see *McGowan v. Maryland*, 366 U.S. 420; and a $1.50 poll tax, *Harper v. Virginia Bd. of Elections*, 383 U.S. 663. . . . As Professor Davis has put it: "The basic idea that comes out in numerous cases is that an identifiable trifle is enough for standing to fight out a question of principle; the trifle is the basis for standing and the principle supplies the motivation."

Three United States courts of appeals have relied on this decision to hold that a mere trifle also suffices under Article III. *LaFleur v. Whitman*, 300 F.3d 256, 270 (2d Cir. 2002); *Sierra Club, Lone Star Chapter v. Cedar Point Oil Co., Inc.*, 73 F.3d 546, 557 (5th Cir. 1996); *Doe v. County of Montgomery, Ill.*, 41 F.3d 1156, 1159–60 (7th Cir. 1994). The time lost by plaintiff establishes a harm for standing purposes.

2. FACEBOOK'S MOTIONS TO STRIKE EXPERT TESTIMONY.

This order now turns to Facebook's two *Daubert* motions to strike expert testimony. Facebook moves to strike all of the various submissions of two of plaintiff's experts. These experts are: (i) Identity Theft Expert James Van Dyke and (ii) CPA Ian Ratner.

A. Identity Theft Expert James Van Dyke.

This order finds that Expert Van Dyke did not base his testimony in sufficient facts or data. Nor is his testimony the product of reliable principles and methods. And even accepting the principles and methods he used, Van Dyke did not reliably apply these methods to the facts of this case.

Expert Van Dyke's 29-page opinion testimony boils down to two conclusions. *First*, [redacted] *Second*, [redacted]

Van Dyke cherry-picked his own prior expert opinions. He recycled a conclusion from a different case. He removed references to a critical premise that does not apply here. More specifically, in Van Dyke's report from the Anthem data breach case, Van Dyke highlighted the importance of social security numbers to identity theft:

> More damaging forms of misuse often result from criminals amassing more elements of any one consumer's data — akin to assembling all pieces of a puzzle, ***with the social security number being a key foundational element***. As an example . . . .

In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2017 WL 3730912 (N.D. Cal. Mar. 21, 2017) (Dkt. No. 744-24 ¶ 19) (emphasis added).

In the report here, Van Dyke cut and pasted the same exact language except *he omitted any reference to Social Security numbers being "key"* to the risk of identity theft described (Van Dyke Decl. ¶ 3.n.):

> More damaging forms of misuse often result from criminals amassing more elements of any one consumer's data — akin to assembling all pieces of a puzzle. As an example . . . .

Plaintiff argues Van Dyke simply took care to omit a fact that did not apply to this case, namely the part about social security numbers. This misses the point. The point is that the social security numbers ranked as "key" — until this case, where they weren't stolen, so the "key" element got removed. This inconsistency means Van Dyke says whatever is convenient to the case at hand.

In addition, Van Dyke's opinions and declarations were riddled with error. His report referred to the theft of maiden names. Maiden names were not taken in the instant breach. He later admitted this inclusion "was a mistake." He also posited that internet protocol addresses were stolen in the attack and spun a hypothetical that depended on a person knowing "the names of family members." He further spent much of his report homing in on the theft of mailing addresses. Yet, to repeat, none of this information was taken in the breach. Moreover, in a separate paragraph in his declaration, he referred to how "victims now suffer reduced value of personal information." This, too, he later walked back, conceding that this paragraph should never have been included. Van Dyke also wrote that he was "retained by [p]laintiffs' counsel in March of 2018" in this case. But this data breach occurred in September 2018. That sequence seems impossible (Van Dyke Decl. ¶¶ 2.a., 3.o, 4.b., 5.d., 5.h., 5.l., 6.p., 6.q., 7.f., 8.a.; Reply Decl. ¶¶ 2.b.ii., 2.g., 2.i.) (Dkt. Nos. 197-32; 231-4).

United States District Court
For the Northern District of California

In a reply declaration, Van Dyke cited to a "beta" "proprietary algorithm" that he claimed generated a "risk level" of 6 out of 10 for the Facebook breach (Reply Decl. ¶ 2.h.). Facebook deposed him. Inexplicably, it then came to light that he also generated this rating by *including information that had not been compromised in the breach* [redacted]. *When the correct information was input instead, the risk level fell to a 1.2 for Group 1 users and* [redacted] Van Dyke II Dep. at 465:18–467:9). According to Van Dyke's own website, less than a two out of ten risk level describes a breach that does not warrant consumer action of any kind (Dkt. No. 248-6). This result squarely conflicts with his expert opinion.

In response to all this, counsel primarily argue that Van Dyke's testimony rested on "his knowledge and experience in the field [of consumer identity fraud]" (Opp. Br. at 9) (Dkt. No. 233). This order presumes Van Dyke is an expert. Yet his report is too flawed. Even a good expert can do a bad job.

The vast majority of the testimony submitted by Van Dyke was boilerplate from other cases. It could have been written about any data breach, and lacked sufficient analysis. It contained too many errors to be relied upon. For the foregoing reasons, Facebook's motion to strike Van Dyke's Report is **GRANTED**.

B. CPA Ian Ratner.

Facebook also challenges the admissibility of CPA Ratner's expert testimony as to his damages analysis. *First*, Facebook argues that he ignores foundational problems in calculating the diminished value of personal information. *Second*, Facebook argues that his time and risk based damages are hypothetical and unreliable. This order disagrees.

"Shaky but admissible evidence is to be attacked by cross examination, contrary evidence, and attention to the burden of proof, not exclusion." *Primiano v. Cook*, 598 F.3d 558, 564 (9th Cir. 2010). As to Facebook's first argument, CPA Ratner attempted to show, through economic models, that access to personal information in-and-of-itself has market value, and that the hackers taking the personal information freely from Facebook is a value lost to the class members (Ratner Decl. ¶¶ 45, 46). He also showed that companies are willing to pay money (such as through targeted advertising) for access to someone's personal information. In addition, he pointed out that Facebook's role in the data breach deprived plaintiff and the class members from being able to control access to their personal information and monetize it if they so chose. This calculation is admissible.

Turning to Facebook's second argument, CPA Ratner attempted to calculate class-wide damages for class members' risk and stress from the breach, time spent dealing with the consequences of it, and the risk of identity theft. Facebook argues that these are mere averages and don't address the characteristics of each class member. "Normally, failure to include variables will affect the analysis' probativeness, not its admissibility." *Hemmings v. Tidyman's Inc.*, 285 F.3d 1174, 1188 (9th Cir. 2002) (quotations omitted). This too must be attacked by cross examination. The motion to strike CPA Ratner's expert opinion is **DENIED**.

3. PLAINTIFF'S MOTION FOR CLASS CERTIFICATION.

Plaintiff moves to certify a damages class under Rule 23(b)(3), an "issues" class under Rule 23(c)(4), and an injunctive-only class under Rule 23(b)(2). Facebook trains most of its fire on the Rule 23(b)(3) class. This order therefore begins there.

A. Rule 23(b)(3).

Before certification, the district court "must conduct a 'rigorous analysis' to determine whether the party seeking certification has met the prerequisites of Rule 23." *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1186 (9th Cir. 2001) (*quoting Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1233 (9th Cir. 1996)). As part of this inquiry, the district court has an obligation to ensure "that a class representative must be part of the class and possess the same interest and suffer the same injury as the class members." *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 156 (1982) (internal quotation marks and citations omitted). This sometimes involves delving into the merits to resolve factual disputes to the extent necessary to determine whether the Rule 23 elements have been met. *See Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350–52 (2011).

Plaintiff Stephen Adkins seeks to represent a nationwide class of Facebook users who had information taken in the data breach. The Terms of Service provide that California law governs both the terms "and any claim, without regard to conflict of law provisions" (Dkt. No. 98-1 § 4.4). Thus, California law applies even as to tort claims, and a nationwide class will not become bogged down in the differences among state laws of negligence. In that connection, plaintiff Adkins, on behalf of the class, seeks to recover on two theories of damages under California law: (i) the cost of a credit monitoring service and (ii) the diminished value of the personal information taken in the breach. This order holds that neither harm presents a cognizable injury, and so the damages class cannot be certified.

i. Credit Monitoring.

Under his first theory of liability, plaintiff Adkins seeks the cost of credit monitoring on behalf of the class. Plaintiff's expert CPA opines that credit monitoring will be appropriate to redress the class's "increased risk, stress, nuisance, inconvenience, and annoyance of identity theft" (Ratner Decl. ¶ 32). Significantly, plaintiff Adkins has never paid any money as a result of this data breach. Had he paid for credit monitoring, for example, he could prevail on this claim. But he has never purchased any credit monitoring service. Plaintiff Adkins's theory of liability instead relies on the aforementioned injuries, like his present stress and the increased risk of identity theft.

While plaintiff Adkins has standing to sue based on his increased risk of future identity theft, in California, this risk alone does not rise to the level of appreciable harm to assert a negligence claim. California has long held that "[i]t is fundamental that a negligent act is not actionable unless it results in injury to another." *Fields v. Napa Milling Co.*, 164 Cal. App. 2d 442, 447 (1958). California also holds that "[n]ominal damages, to vindicate a technical right, cannot be recovered in a negligence action, where no actual loss has occurred." *Id.* at 448. In addition, in a different context, the California Supreme Court has indicated that the mere threat of future harm is insufficient. *See Jordache Enters., Inc. v. Brobeck, Phleger & Harrison*, 18 Cal. 4th 739, 743 (1998).

No binding decision has ever decided whether or not future harms from a data breach can anchor a claim for negligence. In California, such an exception would follow from an already recognized exception to the present harm requirement, namely the cost of future medical monitoring due to an exposure to toxic chemicals. *Potter v. Firestone Tire & Rubber Co.*, 6 Cal. 4th 965, 1009 (1993). The weight of persuasive decisions militates against extending this exception to cases like ours.

In a non-precedential decision, our court of appeals applied Arizona law to reject extending medical monitoring to credit monitoring in a data breach when the plaintiff did not present any actual evidence of identity theft. *Stollenwerk v. Tri–West Health Care All.*, 254 F. App'x 664, 665–67 (9th Cir. 2007). In *Ruiz v. Gap, Inc.*, Judge Samuel Conti relied on *Stollenwerk* to reject that the medical monitoring exception would apply to credit monitoring under California law. Judge Conti opined that medical monitoring was a personal injury permitted to protect public health, but "[t]here is no such public health interest at stake in lost-data cases." 622 F. Supp. 2d 908, 914–15 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689 (9th Cir. 2010). Judge Conti's decision was upheld on appeal on other grounds.

Since these decisions, Judge Gary Klausner and Judge Richard Seeborg have extended the medical monitoring exception to credit monitoring. *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *5 (C.D. Cal. June 15, 2015) (Judge Gary Klausner); *Castillo v. Seagate Tech., LLC*, No. 16-cv-01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) (Judge Richard Seeborg). The undersigned judge would be inclined to follow these decisions and hold credit monitoring available to data breach victims.

Yet, even these decisions cannot help plaintiff Adkins here. Specifically, Judge Klausner permitted "*costs already incurred*, including costs associated with credit monitoring," and specifically dismissed the negligence theory of an increased risk of *future* harm. *Corona*, 2015 WL 3916744, at *4–5 (emphasis added). Judge Richard Seeborg also held that "[t]hose who have incurred such out-of-pocket expenses have pleaded cognizable injuries, whereas those who claim only that they may incur expenses in the future have not." *Castillo*, 2016 WL 9280242, at *4.

United States District Court
For the Northern District of California

This dividing line is further supported by another non-precedential decision by our court of appeals. In *Krottner v. Starbucks, Corporation*, our court of appeals applied Washington law to dismiss a data breach claim for negligence because there was only the *risk* of future identity theft. 406 F. App'x 129, 131 (9th Cir. 2010). Because the claim for negligence could not proceed merely on such risk, our court of appeals expressly did not reach the issue of whether credit monitoring would be appropriate. *Id.* at 131–32. One district judge relied on this decision to dismiss a California negligence claim in the context of a data breach. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 963 n.17 (S.D. Cal. 2012) (Judge Anthony Battaglia) (California and Washington law not "materially different").

So too here. Plaintiff Adkins has incurred zero out-of-pocket expenses as a result of this breach. The time he spent reacting to this data breach may be recoverable as damages in its own right, but has no relationship to the remedy of future credit monitoring. To the contrary, [redacted]

On the evidence presented, therefore, no decision supports that plaintiff Adkins can allege a viable negligence claim under a credit monitoring theory. If some members of the class bought credit monitoring because of this data breach, perhaps they can assert such a claim. Plaintiff Adkins, however, is not a member of the class he seeks to represent. He therefore cannot represent the class on this theory.

ii. Diminished Value of Personal Information.

Two prior orders deemed the harm of diminished value of personal information insufficient to satisfy injury for purposes of Section 17200 and the CLRA (Dkt. Nos. 153, 185). Plaintiff Adkins now asserts an entirely new theory on how to calculate this harm for the negligence claim (Ratner Decl. ¶¶ 45, 46) (emphasis added):

> *[Personal information], such as that maintained by Facebook, derives value from remaining private.* The value of this privacy should be exclusively enjoyed by Facebook's users. However, as a result of the [d]ata

> [b]reach, Facebook essentially granted access to [personal information] for free and conveyed value to unauthorized third parties without compensation to the rightful owners of that information — its users. When the users provided their [personal information] to Facebook, they received the value of Facebook's social media services in return. When Facebook allowed third parties to access the users' [personal information], no value was conveyed to the users. *The value that Facebook's users lost as a result of that conveyance can be measured through the [m]arket [m]ethod (a standard valuation method) by analyzing what third parties pay to access comparable information.*

In other words, plaintiff's injury stemmed from loss of privacy and loss of royalties. Again, however, this calculus is too speculative to assert a claim for negligence. Plaintiff never asserts that he would have paid anyone to access comparable information. Although it's true that each user's information is worth a certain amount of money to Facebook and the companies Facebook gave it to, it does not follow that the same information has independent economic value to an individual user. That Adkins *could* have received royalties is not a cognizable injury.

For these reasons, the Rule 23(b)(3) class is **DENIED**.

B. Rule 23(c)(4).

"When appropriate," Rule 23(c)(4) allows a court discretion to certify an action "as a class action with respect to particular issues." The text does not explain when such a class would be appropriate. Here, plaintiff seeks certification of damages claims for lost time. Duty and breach would be tried on a common basis. Causation and damages would be tried individually. This order agrees with Facebook that "issue certification is not appropriate where the determination of liability itself requires an individualized inquiry" (Dkt. No. 215 at 25 *quoting* 1 *McLaughlin on Class Actions* § 4:43 (15th ed. 2018)). That is, bifurcating elements of liability "does not materially advance the overall disposition of the case because" the court must still consider "plaintiff-specific matters such as fact of injury, causation . . . and extent of damage" (*ibid. quoting McLaughlin*, *supra*). Plaintiff's request to certify an issues-only class under Rule 23(c)(4) is **DENIED**.

C. Rule 23(b)(2).

Class certification is appropriate when a plaintiff can show that all of the prerequisites of Rule 23(a) and one of the requirements of Rule 23(b) has been met. *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1124 (9th Cir. 2017). Rule 23(a) considers whether "(1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class." None of these elements are contested, and this order finds they have been satisfied. Plaintiff stands shoulder to shoulder with other class members when it comes to forward-looking relief. He is typical and adequate.

Rule 23(b)(2) provides that "[a] class action may be maintained if Rule 23(a) is satisfied and if . . . 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." Here, plaintiff seeks injunctive relief to impose a set of changes on Facebook's conduct to ensure no further harm comes to him and the class.

What plaintiff seeks, on behalf of the class is, as follows. *First*, a declaration that Facebook's existing security measures do not comply with its duties of care to provide adequate security. *Second*, to comply with its duties of care, Facebook must implement and maintain reasonable security measures, including that Facebook engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Facebook's systems on a periodic basis, and ordering Facebook to promptly correct any problems or issues detected by such third-party security auditors (Dkt. No. 193 ¶ 221).

In addition, plaintiff seeks an order that Facebook engage third-party security auditors and internal personnel to run automated security monitoring. Any final order may also embed a monitor into Facebook's headquarters. Other requested relief includes: ordering that Facebook audit, test, and train its security personnel regarding any new or modified procedures; ordering that Facebook user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Facebook's systems; ordering that Facebook conduct regular database scanning and securing checks; ordering that Facebook routinely and continually conduct 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; and ordering Facebook to meaningfully educate its users about the threats they face as a result of the loss of their financial and private information to third parties, as well as the steps Facebook users must take to protect themselves (*ibid*.).

Facebook argues that plaintiff does not have standing to allege prospective injunctive relief because Facebook has fixed the bug that caused the data breach. This order holds that Facebook's repetitive losses of users' privacy supplies a long-term need for supervision, at least at the Rule 23 stage. At this stage, there is a likelihood of future harm to warrant potential relief. Plaintiff has standing.

Nor must plaintiffs specify the precise injunctive relief they will ultimately seek at the class certification stage." *B.K. by next friend Tinsley v. Snyder*, 922 F.3d 957, 972 (9th Cir. 2019). Rule 23(b)(2) "[o]rdinarily will be satisfied when plaintiffs have described the general contours of an injunction that would provide relief to the whole class, that is more specific than a bare injunction to follow the law, and that can be given greater substance and specificity at an appropriate stage in the litigation through fact-finding, negotiations, and expert testimony." *Parsons v. Ryan*, 754 F.3d 657, 689 n.35 (9th Cir. 2014).

Here, under these circumstances, the requested relief of an order compelling Facebook to promptly correct any problems or issues detected by such third-party security auditors outlines the "general contours" of the requested injunction at this stage. A more specific remedy can be fashioned later in this litigation. Facebook ultimately has not sufficiently shown otherwise that "crafting uniform injunctive relief will be impossible." *B.K.*, 922 F.3d at 973. Rule 23(b)(2) is satisfied. Plaintiff's motion to certify a Rule 23(b)(2) class is **Granted**.

CONCLUSION

For the foregoing reasons, Facebook's motion to strike Identity Theft Expert James Van Dyke's expert opinion is **GRANTED**. Facebook's motion to strike CPA Ian Ratner's expert opinion is **DENIED**. Plaintiff's motion for class certification of a damages class under Rule 23(b)(3) and under Rule 23(c)(4) is **DENIED**. Plaintiff's motion for class certification of an injunctive class under Rule 23(b)(2) is **GRANTED**.

The following class is **CERTIFIED** for injunctive purposes only: All current Facebook users whose personal information was compromised in the data breach announced by Facebook on September 28, 2018.

This class definition shall apply for all purposes, including settlement. Plaintiff Stephen Adkins is hereby **APPOINTED** as class representative. Plaintiff's counsel Andrew Friedman of Cohen Milstein Sellers & Toll PLLC, John Yanchunis of Morgan & Morgan Complex Litigation Group, and Ariana Tadler of Tadler Law LLP are hereby **APPOINTED** as class counsel. By **DECEMBER 19 AT NOON**, the parties shall jointly submit a proposal for class notification with a plan to distribute notice, including by first-class mail and via Facebook.

This order shall remain redacted for seven calendar days to allow any party an opportunity to seek relief from the court of appeals on the accompanying order on the motions to seal (Dkt. No. 259).

IT IS SO ORDERED.

Dated: November 26, 2019.

WILLIAM ALSUP
UNITED STATES DISTRICT JUDGE