UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

STEPHEN ADKINS, on behalf of himself and those similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

No. C 18-05982 WHA

ORDER GRANTING PRELIMINARY SETTLEMENT APPROVAL

INTRODUCTION

In this data-breach class action, plaintiffs move for preliminary approval of a class settlement agreement. The proposal appearing non-collusive and within the realm of approvable, the motion is **GRANTED**.

STATEMENT

This case arises from the September 2018 hack of Facebook. A prior order detailed the facts (Dkt. No. 153). In brief, certain access tokens permitted access to Facebook users' accounts, but a previously unknown vulnerability made these tokens sometimes visible to strangers. Hackers exploited this flaw in September 2018 to access 300,000 accounts. Once inside, the hackers ran two search queries. 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), including the original 300,000.

In February 2019, five named plaintiffs filed a consolidated complaint asserting several claims. Following consolidation and motion practice, in August 2019, only one named plaintiff, Stephen Adkins, and two claims remained. Six months later, plaintiff Adkins sought to certify a class of affected Facebook users. The motion outlined three classes under Rule 23(b)(2), Rule 23(b)(3), and Rule 23(c)(4). A November 2019 order certified a worldwide class for injunctive purposes only (Dkt. No. 260). One month later, on the parties' motion, a December 19 order limited the injunctive class to users within the United States and removed the requirement of class notice via first-class mail (Dkt. No. 271). The certified class for injunctive purposes only became:

> All current Facebook users residing in the United States whose personal information was compromised in the data breach announced by Facebook on September 28, 2018.

On January 8, under the supervision of Chief Magistrate Judge Joseph Spero, the parties reached a settlement in principle (Dkt. No. 281). During the settlement conference, the parties discussed potential security commitments Facebook could make as part of a settlement. Following those discussions, with the assistance of plaintiff's expert, the parties reached a final set of security commitments and came to a proposed settlement agreement. Plaintiff now moves for preliminary approval of the settlement agreement and to direct notice of the settlement. This order follows briefing and oral argument.

ANALYSIS

Our court of appeals maintains a "strong judicial policy" in favor of settlement of "complex class action litigation." *Class Plaintiffs v. City of Seattle*, 955 F.2d 1268, 1276 (9th Cir. 1992). But a class settlement must offer fair, reasonable, and adequate relief. *Lane v. Facebook, Inc.*, 696 F.3d 811, 818 (9th Cir. 2012). Preliminary approval is appropriate if "the proposed settlement appears to be the product of serious, informed, non-collusive negotiations, has no obvious deficiencies, does not improperly grant preferential treatment to class representatives or segments of the class, and falls within the range of possible approval." *In re*

United States District Court
Northern District of California

Tableware Antitrust Litig., 484 F. Supp. 2d 1078, 1079 (N.D. Cal. 2007) (Chief Judge Vaughn Walker).

The proposed settlement imposes a battery of security commitments to prevent future similar attacks. Facebook will certify that the vulnerability exploited in the breach has been eliminated, that it is no longer possible to generate access tokens in the manner that was done in the breach, and that all access tokens generated through the vulnerability have been invalidated. Then, for the next five years, Facebook will adopt the following security commitments to prevent future attacks:

> (1) Increase the frequency of integrity checks on session updates to detect account compromises.
>
> (2) Implement new tools to detect suspicious patterns in the generation and use of access tokens across Facebook.
>
> (3) Implement new tools to help Facebook promptly contain a security incident involving the improper issuance of access tokens.
>
> (4) Implement automatic alerts for specified types of suspicious activity to ensure prompt response.
>
> (5) Undergo annual SOC2 Type II security assessments.
>
> (6) Limit the capabilities of applications that rely on access tokens.
>
> (7) Eliminate "NoConfidence authentication proofs" and require cryptographic proofs of valid logins before generating credentials.
>
> (8) Employ at least one senior security executive with direct reporting authority and obligations to Facebook's Board of Directors.
>
> (9) Expand the logging of access token generation and use metadate to facilitate the detection, investigation, and identification of the compromise of user access tokens.

Compliance with these commitments will be assessed annually by an "unbiased, independent third-party vendor *selected by Facebook*," though with class counsel's approval. Other than sharing the results with the Court and an expert retained to verify compliance, class counsel will keep the results confidential. For the present purposes, the proposed settlement is adequate.

First, this proposal provides the primary injunctive goal of this suit: elimination of the vulnerability and Facebook's commitment to security measures to protect not just class

United States District Court
Northern District of California

members but all Facebook users' personal information. Seven of the nine commitments reflect voluntary measures implemented in response to the breach intended to detect, investigate, contain, and prevent access-token theft or abuse. The remaining two (numbers 5 and 8) reflect previously existing practices that Facebook has committed to continuing as part of the proposal. Following the hearing, Facebook submitted a sworn declaration verifying that none of the security measures have been undertaken as a result of any other court order or regulatory directive.

Second, the proposal ensures Facebook's commitment to these measures for the next five years under external assessment. Given Facebook has already voluntarily implemented the security measures, this external oversight becomes the real value for the class. Facebook will provide the results of the security assessment to class counsel, a third-party expert, and the Court. Moreover, the ongoing review ensures the continued efficacy of the agreement. Should legal or technological developments render any provision of the proposal obsolete, the parties will work to update the settlement agreement.

Third, the proposal appears to be the product of serious, non-collusive negotiations. Class counsel's fees and costs, and Mr. Adkins's service award are appropriately reserved for the Court's discretion at final approval. Facebook may oppose counsel's fee request and, given the relief here is injunctive, class counsel's fee will not detract from plaintiffs' recovery. The proposed scope of waiver is adequately narrow. Plaintiffs agree to waive all injunctive or declaratory relief claims made in this case, but retain all claims for damages, with the exception of plaintiff Adkins, who releases all claims in exchange for his service award. And, as it provides for uniform injunctive relief, the proposal treats class members equitably relative to each other.

Fourth, notice to the class is "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections." *Mullane v. Central Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). A prior order approved the notice program (Dkt. No. 271). Class notice will be distributed via the email addresses linked to the class members' Facebook accounts, via reverse

United States District Court
Northern District of California

phone look-up to identify the few Facebook users who did not input their email address, a dedicated website, social media campaigns, internet banner ads, and a traditional media campaign. Counsel have selected Angeion Group, whom the undersigned has recently approved as administrator in another case, as the class administrator here. *See In re Glumetza Antitrust Litigation*¸ No. C 19-05822 WHA, Dkt. No. 389 (N.D. Cal. Oct. 15, 2020).

Following the hearing, the parties have appropriately simplified the process for plaintiffs to object to the proposed settlement. However, the proposed notice requires three more minor changes. Counsel shall please clarify that a class member need only mail an objection letter to *one* of the several addresses for the class administrator and class counsel. Then, given the impact of COVID-19, the proposed notice shall please indicate both that the final approval hearing may take place telephonically and that the Clerk's office hours have also been impacted. If in the coming months it appears that an in-person fairness hearing will be out of the question due to public health, the Court will appreciate counsel's assistance in providing a certain number of class members the opportunity to speak at the hearing by phone, should they wish.

* * *

The parties seek to seal several documents submitted in support of the proposed settlement (Dkt. Nos. 280, 296, 299). Public policy heartily favors openness in our court system as the public is entitled to know to whom we are providing relief (or not). *See Kamakana v. City & Cty. of Honolulu*, 447 F.3d 1172, 1179–80 (9th Cir. 2006). Generally, "a court may seal records only when it finds a compelling reason and articulates the factual basis for its ruling, without relying on hypothesis or conjecture." *Ctr. for Auto Safety v. Chrysler Grp.*, 809 F.3d 1092, 1096–97 (9th Cir. 2016) (quotations and citations omitted).

Facebook asserts that malicious actors with public access to this information could leverage it to evade Facebook's security systems and circumvent detection, endangering user information. The redactions are limited to specific testing parameters and triggering events that, although important, are not so determinative of the relief afforded that a meaningful evaluation of the proposal cannot be made without them. Against the risk of endangering the user

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

Smarter legal research.