ALTSHULER BERZON LLP
EVE CERVANTEZ (SBN 164709)
ecervantez@altshulerberzon.com
JONATHAN WEISSGLASS (SBN 185008)
jweissglass@altshulerberzon.com
DANIELLE E. LEONARD (SBN 218201)
dleonard@altshulerberzon.com
MEREDITH A. JOHNSON (SBN 291018)
mjohnson@altshulerberzon.com
TONY LOPRESTI (SBN 289269)
tlopresti@altshulerberzon.com
177 Post Street, Suite 300
San Francisco, CA 94108
Telephone: (415) 421-7151
Facsimile: (415) 362-8064

COHEN MILSTEIN SELLERS & TOLL PLLC
ANDREW N. FRIEDMAN (admitted pro hac vice)
afriedman@cohenmilstein.com
GEOFFREY GRABER (SBN 211547)
ggraber@cohenmilstein.com
SALLY M. HANDMAKER (SBN 281186)
shandmaker@cohenmilstein.com
ERIC KAFKA (admitted pro hac vice)
ekafka@cohenmilstein.com
1100 New York Ave. NW
Suite 500, West Tower
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

Lead Plaintiffs' Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

In Re Anthem, Inc. Data Breach Litigation	Case No. 15-MD-02617-LHK **PLAINTIFFS' MEMORANDUM IN SUPPORT OF FINAL APPROVAL OF CLASS ACTION SETTLEMENT** Date: February 1, 2018 Time: 1:30 p.m. Judge: Hon. Lucy H. Koh Crtrm: 8, 4th Floor

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

I. INTRODUCTION

When Plaintiffs moved for preliminary approval, they addressed each of the "*Churchill* factors" that would apply at the final approval stage. The Court granted Plaintiffs' motion for preliminary approval, but not before an hour-long hearing where the Court conducted a wide-ranging inquiry into the merits of the Settlement, actively engaged with Class Counsel and counsel for the Defendants, and considered concerns raised by counsel for certain named plaintiffs. *See* 8/17/16 Hr'g Tr. [ECF 897]; 8/25/17 Order [ECF 903]. In response to the Court's suggestions, the parties amended the proposed Settlement Agreement, clarifying the scope of the release, and revised the class notices and related communications. *See* ECF 900.

The settlement now comes before the Court again, this time for final approval. If approved, it would require Anthem to establish a record $115 million settlement fund – far more than any other data breach defendant has paid to date. That fund will be used to purchase credit monitoring services to protect class members from fraud and ensure that any identity theft is detected and remedied quickly; to provide alternative compensation of up to $50 per class member; and to pay out-of-pocket expenses incurred as a result of the data breach. The retail value of the credit monitoring (purchased in bulk at a discount) is billions of dollars for the entire class, or, conservatively, over $213 million to the 891,431 class members who have claimed credit monitoring thus far. Anthem will also be required to spend at least [redacted] to help protect class members' personal information over the next three years – an increase of [redacted] over pre-breach spending – and to implement or maintain specific changes to its data security practices, including encryption of personally identifiable information ("PII") and archiving of older data with strict access controls.

The Settlement Administrator has mailed class notice to 54.9 million class members; e-mailed notice to 5.15 million class members; published notice in two leading consumer magazines; and disseminated over 180 million internet advertisements on sites like Twitter, Facebook, and Google, to further apprise class members of their rights under the settlement. Class members and the public at large have responded with a great deal of interest. The national media has reported on the settlement, over 850,000 people have visited the Settlement Website, and more than 80,000

have called the Settlement Administrator's automated phone line for more information. Over a million class members have already submitted claims to participate in the settlement, while only eight have objected to or commented on the settlement, and only 169 have requested to opt out of the settlement. Class members have until December 29 to submit objections and opt-out requests, and until January 29 to submit claims, so it is too soon to fully assess the class's reaction to the settlement. But early indications are that the settlement has widespread support, and the other *Churchill* factors continue to favor settlement approval.

By settling now, class members can obtain timely and practical remedies that otherwise would not be available for years, if at all. What typical class members want most is for their private information to remain confidential and secure. Extended credit monitoring services and immediate changes to Anthem's data-security practices can help achieve that goal. Credit monitoring works to prevent and detect misuse of information taken in the data breach, while changes in data-security practices work to reduce the risk of future breaches. Credit monitoring services are needed most in the first four to five years after a data breach occurs, and security measures are most effective the sooner they can be implemented. This is a case, in other words, where delay would have hurt class members. Plaintiffs accordingly move for final approval of the Settlement on the same grounds that they sought and obtained preliminary approval – grounds that are reiterated below for the Court's and class members' convenience.

II. BACKGROUND

A. Plaintiffs' Claims

In early 2015, Anthem acknowledged that it had been the target of a cyberattack and that information related to approximately 78.8 million people had been compromised. Names, dates of birth, Social Security numbers, and health care ID numbers were among the stolen data. Anthem offered those affected by the data breach two years of credit monitoring, but denied that the stolen information had ever been misused.

Over 100 lawsuits were filed and centralized before this Court for pre-trial proceedings, and several hundred claims arising out of the laws of all 50 states were researched and consolidated into a single complaint. Fourth Consol. Am. Compl. [ECF 714-4]. Plaintiffs' claims

follow diverse legal paths to recovery, but all of them begin with the same premise: that Anthem's data security was inadequate. Plaintiffs' case depended, above all, on proving their allegations that the data breach was possible only because Anthem had aggregated almost 80 million people's private information into a central data warehouse that was not properly secured. On behalf of those individuals, Plaintiffs sought both equitable and monetary relief.

1. Equitable Remedies

Plaintiffs requested several types of equitable relief. The first was aimed at reforming Anthem's data security. Mot. for Class Cert. ("Class Cert.") [ECF 743-12] at 10-11. Plaintiffs submitted expert analysis setting forth several security controls needed to protect the private information already stored by Anthem into the future. Strebe Report [ECF 744-17] at 73-82. Had the case not settled, Plaintiffs planned to request that the Court enter an injunction requiring Anthem to implement those additional measures and also to maintain the security reforms that Anthem had already begun during the litigation. *See* Cervantez Decl. ¶ 5.

The second form of equitable relief Plaintiffs sought was extended credit monitoring. Shortly after acknowledging the data breach, Anthem offered class members two years of AllClear single-bureau credit monitoring and identity repair services. *See* Opp. to Mot. for Class Cert ("Class Cert Opp.") [ECF 797-8] at 3. That credit monitoring has expired for the class, however, and because Plaintiffs' expert has explained that it is important to protect against identity theft or other forms of fraud with credit monitoring for the first five years following a data breach, Plaintiffs sought additional credit monitoring. Class Cert. at 10; Van Dyke Report [ECF 744-25] ¶ 46. Plaintiffs also requested, on the advice of their expert, credit monitoring more extensive than the AllClear services offered by Anthem, including triple-bureau credit monitoring and identity validation monitoring. Van Dyke Report ¶ 50(b); *see also* Cervantez Decl. ¶ 5.

Because not all class members were Anthem insureds, presenting privity and other potential defenses to certain claims, Plaintiffs also named The Blue Cross and Blue Shield Association ("BCBSA") and 17 non-Anthem Blue Cross Blue Shield companies as co-defendants with Anthem, to ensure that these class members would be entitled to monetary remedies for breach of contract and state consumer protection act statutes. Plaintiffs also sought to ensure that

these other BCBSA licensees employ adequate security measures before conveying their insured's private information to other licensees such as Anthem. Following the public announcement of the Anthem data breach, the BCBSA Membership Standards were amended to further define certain guidelines for the protection and cybersecurity of personal information. *See* Cervantez Decl. ¶ 7. For settlement purposes, Plaintiffs determined that this change sufficiently addressed their concerns. *Id.*

2. Monetary Remedies

Plaintiffs requested monetary relief in the Complaint under three theories of damages: Benefit of the Bargain, Loss of Value of Personally Identifiable Information, and Consequential Out-of-Pocket Expenses. *See* 2nd MTD Order [ECF 524] at 22-29. The Benefit of the Bargain theory of damages would compensate class members based on the difference in value between the health insurance Anthem should have provided (which would have included adequate data security) and the value of the health insurance that Anthem actually provided (which Plaintiffs allege lacked adequate data security). Class Cert. at 12. Plaintiffs have proposed isolating the value of adequate data security through a conjoint analysis, which would use surveys and statistical analyses to estimate how consumers value different product attributes. *Id.*; Rossi Report [ECF 744-22] ¶ 14. Plaintiffs' expert was prepared to complete the conjoint surveys after one or more classes were certified by the Court. *See* Cervantez Decl. ¶ 6.

The Loss of Value of PII theory approaches damages from a different direction, and attempts to measure the economic cost of losing the confidentiality of one's private information. One way of doing this is to look at the price for certain types of PII on the black market. Plaintiffs' expert put that price at a minimum of $10 per individual, while Defendants' expert placed it at $4 per individual. Class Cert. at 13. Another way to measure Loss of Value of PII is to look at the retail price of products that protect data-breach victims from identity fraud. Plaintiffs' expert put that cost at $9 to $20 per month for five years. Class Cert. at 13; Van Dyke Report ¶ 53.

Plaintiffs' third measure of damages – the Consequential Out of Pocket Expenses theory – would allow class members to recover any out-of-pocket expenses they incurred as a result of the data breach. These costs include unreimbursed fraud losses, money and time spent to rectify

identity fraud, and fees for fraud-prevention and detection services. Class Cert. at 22. Unlike the other measure of damages, however, the evidence needed to prove out-of-pocket damages is in class members' possession and would need to be set forth on an individualized basis. *Id.* at 22-23.

In addition to Plaintiffs' three theories for assessing class members' actual damages, some of Plaintiffs' claims authorized statutory damages. For example, the New York GBL § 349 claim at issue in Plaintiffs' pending motion for class certification provides for an award of $50 per violation or actual damages, whichever is greater. N.Y. Gen. Bus. Law § 349(h).

B. History of the Litigation and Settlement Negotiations

After Plaintiffs' lawsuits were centralized and their claims consolidated into a single complaint, the Court implemented a bellwether process to adjudicate those claims. ECF 326 at 2-3. Five claims chosen by Plaintiffs and five chosen by Defendants were subjected to two rounds of briefing on the pleadings. Four of the ten claims were dismissed (Indiana negligence, Kentucky consumer protection, Kentucky data breach, and Georgia insurance privacy), while the remaining six claims largely survived (California, New Jersey, and federal breach of contract, California and New York consumer protection, and New York unjust enrichment). *See* Order on 1st MTD [ECF 468]; Order on 2nd MTD [ECF 524].

The parties have now fully briefed class certification and related *Daubert* motions. Plaintiffs have also reviewed 3.8 million pages of documents; litigated 14 discovery motions; deposed 18 percipient fact witnesses, 62 corporate designees, and six expert witnesses; produced over 100 plaintiffs and four expert witnesses for deposition (with 29 of the plaintiffs also producing their computers for forensic imaging); and exchanged 76 interrogatories, 731 RFAs, and 18 expert reports with Defendants. Cervantez Decl. ¶ 3. Plaintiffs' extensive discovery provided them with a deep understanding of Anthem's highly-complex IT systems, the numerous technical and administrative controls involved in Anthem's data security system, and the deficiencies within that system that Plaintiffs allege contributed to the data breach and should be remedied. *Id.* ¶ 19.

While the parties were briefing class certification, they were also engaging in a series of mediation sessions with Judge Layn R. Phillips (Ret.). *Id.* ¶ 4. After three full-day mediations over the course of three months – on February 28, April 20, and May 22, 2017 – the parties still

had not reached a deal. *Id.* Judge Phillips ultimately made a mediator's proposal, which both sides accepted over Memorial Day weekend. *Id.*

C. Overview of the Settlement

1. The Proposed Settlement Class

If approved, the parties' settlement would offer relief to the following proposed class:

> Individuals whose Personal Information was maintained on Anthem's Enterprise Data Warehouse and are included in Anthem's Member Impact Database and/or received a notice relating to the Data Breach; provided, however, that the following are excluded from the Settlement Class: (i) Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns; (ii) any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff; and (iii) any individual who timely and validly opts-out from the Settlement Class.

Cervantez Decl., Ex. 11 ("SA") ¶ 1.36. This proposed class covers the approximately 78.8 million individuals whose personal information was compromised by the Anthem data breach, and parallels the class definitions suggested in Plaintiffs' Fourth Amended Complaint and motion for class certification, although it does so through a single nationwide class rather than a series of state-wide classes.

2. Changes to Anthem's Data Security Practices

One of the primary benefits of the proposed settlement is that it requires Anthem to improve its data security. In the years before the breach, Anthem was devoting approximately [redacted] per year to information security. Cervantez Decl. ¶ 12. It will now be required to spend at least [redacted] per year over the next three years – an increase of [redacted] over Anthem's pre-breach allocation. Settlement Ex. 2 [ECF 869-11] ¶ 8. Anthem will also be required to deploy specific cybersecurity measures, including encrypting PII and archiving certain databases with strict access controls. In particular, Anthem must:

(1) immediately implement [redacted] and [redacted], including [redacted];

(2) remove PII in the database that was the subject of the breach no more than [redacted] years after it enters the database;

(3) [redacted];

(4) implement additional levels of management approval [redacted];

(5) require use of [redacted];

(6) [redacted];

(7) undertake an annual security risk assessment using an outside third party;

(8) conduct [redacted] at least twice per year; and

(9) conduct ongoing [redacted] within a set time period.

Id. ¶¶ 1-3, 7 10-11. These measures were derived in consultation with security experts based on Plaintiffs' extensive discovery, and squarely address the inadequate security that Plaintiffs had focused on in the litigation. *See* Class Cert. at 3-4; Cervantez Decl. ¶ 19.

To ensure that Anthem maintains these enhanced security measures, and that the measures are operating effectively, Anthem will be required both to retain independent consultants to undertake an annual IT security risk assessment and an annual settlement compliance review, and to provide the results of the annual settlement compliance review and its annual SOC 2 Type 2 assessment to Plaintiffs' counsel for review. SA ¶¶ 2.3-2.4; Settlement Ex. 2 [ECF 869-11] ¶ 7. And whereas Plaintiffs contend Anthem previously failed to spend the money required to address potential vulnerabilities identified internally or by outside auditors, Anthem will now be required to follow specific remediation schedules to address potential vulnerabilities. Settlement Ex. 2 [ECF 869-11] ¶¶ 9 & 11. The proposed settlement thus ensures that Anthem will adapt to changing cybersecurity threats as they emerge.

These immediate fortifications to Anthem's systems represent significant improvements in Anthem's security practices, and move substantially towards remedying the many security issues Plaintiffs identified as deficient. Although Anthem's specific obligations under this part of the settlement necessarily expire after three years because the pace of technology and evolving security standards make it difficult to prescribe appropriate measures on a longer-term basis, the settlement is formulated to ensure that Anthem not only deploys the up-front resources needed to address existing security vulnerabilities, but institutionalizes the consistent costs, practices, and accountability needed for long-term, proactive data security. In addition, the cost and public

nature of this litigation serve as long-term incentives for Anthem to continue deploying appropriate data security.

3. Settlement Fund

In addition to addressing the security deficiencies that Plaintiffs believe contributed to the data breach, and ensuring that Anthem takes proactive measures to prevent against future attacks, the proposed settlement requires Anthem to pay $115 million into a Qualified Settlement Fund. SA ¶ 3.1. The Settlement Fund will be used in the following manner:

a) Fraud Protection and Credit Monitoring

Settlement funds will first be used to pay for at least two years of identity fraud prevention and detection services for class members who file claims. Experian has worked with Plaintiffs' counsel to create a custom product designed specifically to provide protection against the particular threats facing class members, based on the type of PII exfiltrated in the Anthem data breach. Cervantez Decl. ¶ 8. The product is based on the recommendations submitted by Plaintiffs' expert in support of class certification (*see* Van Dyke Report ¶ 52), and includes:

(a) daily monitoring of class members' credit files at all three major credit reporting agencies to detect suspicious activity (such as applications for loans or credit not initiated by the class member);

(b) internet surveillance, including monitoring the "dark web" to detect the covert sale of class members' PII;

(c) identity validation monitoring to notify class members if their identity is used to open a new account or to perform an identity validation within the Experian network;

(d) identity theft insurance, which covers designated identity theft related expenses, including unreimbursed fraud losses and professional services, up to $1 million;

(e) Experian credit reports available upon request; and

(f) specific services for class members who are minors, including social security number tracing and internet surveillance.

SA ¶ 4.1; Cervantez Decl. ¶ 8.

By purchasing credit monitoring services in bulk at a discount, the Settlement is able to provide very valuable services to class members. Although the custom product offered to class members is not available to the public, it includes many of the services offered in Experian's retail

"IdentityWorks Premium" product which is sold to the public for $19.99 per month, and more services than Experian's "IdentityWorks Plus" plan, which retails for $9.99 per month. Cervantez Decl. ¶ 9, Ex. 13. Assuming conservatively that the value of the Anthem-specific custom product is only $9.99 per month, the credit monitoring portion of the settlement provides a total value to each class member of $239.76 over the course of 24 months (or up to $479.52 should there be sufficient settlement funds remaining to pay for an additional 24 months of credit monitoring). In other words, the total value of the credit monitoring package offered to the class is worth billions ($9.99 x 24 x 79,150,000). Even using only the number of claims for credit monitoring that have been filed to date (891,431) – a conservative approach, given that the claims deadline is not until January 29, 2018 – the credit monitoring portion of the settlement has provided a value of at least $213 million to the class.

b) Alternative Compensation

Class members who already have credit monitoring services can instead select alternative cash compensation. SA ¶ 5.1. To request this alternative compensation, class members need only submit a simple online claim form confirming the timing and type of their current credit monitoring services. *Id.* ¶ 5.2. After all other claims, fees, and expenses are paid, the Net Settlement Fund will be used to distribute up to $36 to these class members (to be reduced *pro rata* if necessary). *Id.* ¶ 5.3. In addition, if the total amount of these claims is less than $13 million, the amount distributed will be increased on a *pro rata* basis, until it reaches either $50 per person or $13 million in the aggregate. *Id.*

c) Out-of-Pocket Costs

The Settlement Administrator will reserve $15 million from the Settlement Fund to compensate class members who incurred out-of-pocket costs or spent time as a result of the data breach. SA ¶ 6.4. Reimbursable expenses may include unreimbursed fraud losses; time spent remedying issues related to the breach, at $15 per hour or the value of the class members' actual lost wages, whichever is greater; professional fees incurred in connection with identity theft or falsified tax returns; the cost of credit freezes, or of credit monitoring ordered between February

2015 and the date credit monitoring becomes available under the Settlement; and miscellaneous expenses, such as notary, fax, postage, copying, mileage and long-distance charges. *Id.* ¶ 1.23.

Class members can submit claims for up to $10,000 by completing a simple claim form, accompanied by an attestation regarding the expenditures incurred and simple documentation (i.e. letter from IRS if claiming IRS tax fraud expenses). *Id.* ¶ 6.4; Geraci Decl., Ex. I. So long as the claimed fraud is fairly traceable to the Anthem Data Breach (meaning it involved possible misuse of the type of personal information accessed in the Data Breach), Settlement Class Members will not have to prove "causation" – i.e., that the claimed fraud stemmed from the Anthem data breach as opposed to from some other breach. SA ¶¶ 1.23, 6.3. This is a significant benefit to class members, as proving "causation" could be insurmountable in many cases.

The Settlement Administrator will review all submitted claims and will have authority to determine whether and to what extent a claim for out-of-pocket costs is valid. SA ¶ 6.2. If the amount of valid claims submitted on or before the Settlement's Effective Date exceeds $15 million, those claims will be subject to a pro rata reduction. *Id.* ¶ 6.4. Otherwise, the Settlement Administrator will continue to accept and process claims for one year after the Court's final approval order is entered, or until the $15 million reserve is exhausted, whichever comes first. *Id.* ¶¶ 6.1, 6.4. In the event the $15 million reserve is exhausted, the Settlement Website will be updated to inform class members that claims for out-of-pocket expenses will no longer be processed or paid. *Id.* ¶ 6.4.

d) Class Notice and Settlement Administration

Due to the large size of the class and the importance of encouraging class members to sign up for credit monitoring services, the costs of notice and settlement administration have been substantial and are expected to reach approximately $23 million. Cervantez Decl. ¶ 13. In addition to mailing postcard notice to 54.9 million class members with a known mailing address, emailing notice to 5.15 million class members with a known email address, and publishing notice in *People* and *Good Housekeeping*, the proposed settlement provides for an expansive, targeted social media advertisement campaign that included the purchase of 180 million advertising "impressions" spread across Twitter, LinkedIn, Google Display Network, and Facebook. Geraci

Decl. ¶¶ 10-16, Exs. C-F. The advertisements link to the settlement website, where people can enter their name and date of birth to determine whether they are a class member, and then file a claim for credit monitoring services or other settlement benefits. *Id.* ¶¶ 15, 17, Ex. F. This social media campaign is specifically designed to reach the over 23 million people for whom Anthem did not have contact information and who may not have learned that they were victims of the breach and are class members in this litigation. Cervantez Decl. ¶ 13.

The claims process is designed to be easy and accessible. Class members can claim credit monitoring simply by signing and returning the tear-off portion of their postcard notice. Geraci Decl., Ex. C. They may also file claims online at www.DataBreach-Settlement.com, which has been optimized for mobile devices and includes helpful instructional videos. *Id.* ¶ 18. Claims for credit monitoring or alternative compensation can be filed until January 29, 2018, and claims for out-of-pocket compensation can be filed up to a year after final approval (provided the $15 million reserve is not first exhausted). SA ¶¶ 4.3, 6.1. In addition, if Class Members experience identity theft or fraud at any time while Credit Services are being offered, they will be eligible for fraud-resolution services from a trained Experian fraud resolution specialist – even if they did not file a claim for credit monitoring. *Id.* ¶ 4.9.

e) Attorneys' Fees, Costs, and Service Awards

Plaintiffs are separately petitioning the Court for awards of attorneys' fees, costs, and service payments to be paid out of the Settlement Fund. The maximum amounts that Plaintiffs may seek were negotiated with Defendants as part of the Settlement, and as a result, Defendants have agreed not to oppose Plaintiffs' application. SA ¶¶ 11.1, 12.1.

f) Residual Distribution

In no event will any of the Settlement Fund revert to Defendants. Instead, it will be used to extend the duration of the credit monitoring provided to class members for up to two additional years. SA ¶ 4.8. If the residual funds are insufficient to pay for at least one additional month of credit monitoring, or if there are funds remaining after credit monitoring is extended to a total of four years, the remainder will be distributed *cy pres* to the Center for Education and Research in Information Assurance Security (CERIAS) and the Electronic Frontier Foundation. SA ¶ 7.1.

CERIAS is a national center for research and education in areas of information security, while the Electronic Frontier Foundation is a nonprofit organization that champions user privacy. *See* https://www.cerias.purdue.edu/about; https://www.eff.org/about. These two entities are appropriate recipients of *cy pres* awards because their missions are related to the class's interests and they take into account the nationwide geographic scope of the class.

4. Release

In exchange for the benefits provided under the Settlement, Settlement Class Representatives and Settlement Class Members will release any legal claims that may arise from or relate to the facts alleged in the complaints filed in this litigation.[1] *See* SA ¶¶ 1.32 & 13.1-13.3. Pursuant to the Court's suggestions at the preliminary approval hearing, the release has been clarified to explain that Settlement Class Members are *not* releasing claims with respect to either the original cyber attackers who stole Class Members' personal information from Anthem, or from any other person or entity who intentionally misuses that stolen PII for unlawful purposes. 8/24/17 Suppl. Brief [ECF 900]; Cervantez Decl., Ex. 12.

III. ARGUMENT

A. The Settlement Class Satisfies Rule 23

In its preliminary approval order, the Court found that the Settlement Class met the requirements of Rule 23 and preliminarily certified it under Rule 23(b)(3). 8/25/17 Order [ECF 903] ¶¶ 5-7. Plaintiffs now request that the Court affirm its preliminary findings and render a final decision as to the appropriateness of class certification.

1. The Class Meets The Requirements of Rule 23(a)

The prerequisites for class certification under Rule 23(a) are numerosity, commonality, typicality, and adequacy – each of which is satisfied here. Fed. R. Civ. P. 23(a).

The proposed settlement class, set forth above in Section II.C.1, includes approximately 79.15 million people, and so readily satisfies the numerosity requirement. *See* Fed. R. Civ. P. 23(a)(1). The proposed class also satisfies the commonality requirement of Rule 23(a), which

[1] In MDL proceedings, it is proper to release claims based on facts alleged in the underlying MDL complaints. *See, e.g., In re: Volkswagen "Clean Diesel,"* Case No. 3:15-md-02672-CRB, ECF 3230 at 5-6 (N.D. Cal. May 17, 2017).

requires that class members' claims "depend upon a common contention," of such a nature that "determination of its truth or falsity will resolve an issue that is central to the validity of each [claim] in one stroke." *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011). The central question behind every claim in this litigation is whether Anthem adequately secured its data warehouse where class members' personal information was stored. *See* Class Cert at 6-7; Class Cert Reply [ECF 832-6] at 2-5. The answer to that question depends on common evidence that does not vary from class member to class member, and so can be fairly resolved – whether through litigation or settlement – for all class members at once. *See id.*

The final requirements of Rule 23(a) – typicality and adequacy – are likewise satisfied. The proposed class representatives each had personal information that was stored on Anthem's data warehouse and was exfiltrated during the data breach, and so were affected by the same inadequate data security that Plaintiffs allege harmed the rest of the class. *See* Class Cert. at 7-9; *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1118 (9th Cir. 2017) ("it is sufficient for typicality if the plaintiff endured a course of conduct directed against the class"). The proposed class representatives also have no conflicts with the class; have participated actively in the case, including by sitting for depositions and – for many of them – allowing their personal computers to be examined; and are represented by experienced attorneys who were previously appointed by the Court to represent class members' interests. *See* Class Cert. at 7-9; *Staton v. Boeing Co.*, 327 F.3d 938, 957 (9th Cir. 2003) (adequacy satisfied if plaintiffs and their counsel lack conflicts of interest and are willing to prosecute the action vigorously on behalf of the class).

2. <u>The Class Meets The Requirements Of Rule 23(b)(3)</u>

"In addition to meeting the conditions imposed by Rule 23(a), the parties seeking class certification must also show that the action is maintainable under Fed. R. Civ. P. 23(b)(1), (2) or (3)." *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1022 (9th Cir. 1998). Here, the proposed class is maintainable under Rule 23(b)(3), as common questions predominate over any questions affecting only individual members and class resolution is superior to other available methods for a fair resolution of the controversy. *Id.* Plaintiffs' liability case depends, first and foremost, on whether Anthem used reasonable data security to protect their PII. *See* Class Cert. at 11-13; Class Cert.

Reply at 9-11. That question can be resolved using the same evidence for all class members, and thus is the precise type of predominant question that makes a class-wide adjudication worthwhile. *See Tyson Foods, Inc. v. Bouaphakeo*, 136 S. Ct. 1036, 1045 (2016) ("When 'one or more of the central issues in the action are common to the class and can be said to predominate, the action may be considered proper under Rule 23(b)(3) …'").

Certification is particularly appropriate in this context because manageability considerations do not need to be taken into account: "the proposal is that there be no trial," and so manageability considerations have no impact on whether the proposed settlement class should be certified. *Amchem Prods. v. Windsor*, 521 U.S. 591, 620 (1997). There is only the predominant issue of whether Anthem properly secured the personal information taken from its data warehouse, such that Anthem's security should be improved and class members affected by the data breach provided with a remedy. As a practical matter, that issue cannot be resolved through individual trials or settlement negotiations: the amount at stake for individual class members is too small, the technical issues involved are too complex, and the required expert testimony and document review too costly. *See Just Film*, 847 F.3d 1108 at 1123. A class action is thus the superior method of adjudicating consumer claims arising from this data breach – just as in other data breach cases where a class-wide settlement has been approved. *See, e.g., In re Linkedin User Privacy Litig.*, 309 F.R.D. 573, 585 (N.D. Cal. 2015); *In re the Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 6902351, at *2 (N.D. Ga. Aug. 23, 2016); *In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, 2009 WL 5184352, at *6–7 (W.D. Ky. Dec. 22, 2009).

B. The Settlement Merits Final Approval

A proposed class action settlement may be approved if the Court, after allowing absent class members an opportunity to be heard, finds that the settlement is "fair, reasonable, and adequate." Fed. R. Civ. P. 23(e)(2). When assessing a proposed settlement, "the court's intrusion upon what is otherwise a private consensual agreement negotiated between the parties to a lawsuit must be limited to the extent necessary to reach a reasoned judgment that the agreement is not the product of fraud or overreaching by, or collusion between, the negotiating parties, and the

settlement, taken as a whole, is fair, reasonable and adequate to all concerned." *Rodriguez v. West Publ'g Corp.*, 563 F.3d 948, 965 (9th Cir. 2009) (internal quotation omitted).

To assess whether a settlement merits final approval, courts in this Circuit typically consider the following factors:

(1) the strength of the plaintiff's case;
(2) the risk, expense, complexity, and likely duration of further litigation;
(3) the risk of maintaining class action status throughout the trial;
(4) the amount offered in settlement;
(5) the extent of discovery completed and the stage of the proceedings;
(6) the experience and views of counsel;
(7) the presence of a governmental participant;
(8) the reaction of the class members to the proposed settlement; and
(9) whether the settlement is a product of collusion among the parties.

Churchill Vill., L.L.C. v. Gen. Elec., 361 F.3d 566, 575-76 (9th Cir. 2004); *In re Bluetooth Headset Products Liab. Litig.*, 654 F.3d 935, 946 (9th Cir. 2011). As discussed in the sections that follow, an analysis of these factors shows this settlement to be advantageous to the class and worthy of judicial approval.

1. The Strength of Plaintiffs' Case

Plaintiffs believe they have built a strong case for liability. As detailed in their class certification papers and discussed briefly above, the evidence suggests Anthem failed to take a number of industry-standard measures to secure the private information stored in its data warehouse; that Anthem ignored warnings and underfunded its data security; and that Anthem missed numerous opportunities to detect and stop hacker activity while the data breach was underway. *See* Class Cert at 2-4. The liability case is not ironclad, however. Anthem argued that it had assembled a robust IT security program that had a track record of warding off attempted attacks and had been lauded by independent cybersecurity organizations. *See* Class Cert. Opp. at 3-5. It characterized the data breach as an unstoppable state-sponsored attack that used never-before-seen technology, and pointed out that Anthem's quick response to the attack had earned praise from federal officials and industry experts. *Id.* Plaintiffs believe they have answers to those

contentions (*see* Class Cert Reply at 4-5), and a reasonably good chance of proving that Anthem's data security was inadequate. Plaintiffs further believe that if they establish that central factual issue, Anthem is likely to be found liable under at least some of the liability theories and state laws Plaintiffs had pled in their complaint.

Plaintiffs believe their damages theories also stand a good chance of succeeding in some form, as they had withstood vigorous legal challenges at the motion-to-dismiss stage and Plaintiffs had supported the theories with reports from highly qualified expert witnesses. The range of potential outcomes is large, however. Anthem had challenged both the Benefit of the Bargain theory and the Loss of Value of PII theory through *Daubert* motions, and also raised additional legal and factual arguments regarding Plaintiffs' damages theories. Further, while Plaintiffs' theories were sound in principle, their application to data breach litigation was untested beyond the pleading stage. Cervantez Decl. ¶ 18. The scope of damages depended in large part on the scope of class certification, which had yet to be decided. *Id.* The Benefit of the Bargain theory depended upon the results of a conjoint study that could not be completed until after class certification, and there was no guarantee that Plaintiffs would ultimately have found this type of damage at all. *Id.* And it is possible that both the Benefit of the Bargain theory and the Loss of Value of PII theory could yield large numbers that would be unpalatable to a jury. *Id.* If applied across all potential class members, Plaintiffs' most conservative measure (based on black-market rates of at least $4 per individual) would yield a figure of $316 million or more, while the most expansive measure (based on at least $9 of monthly credit monitoring costs) would yield much higher numbers. While the legal theory behind the larger numbers may be sound, it is untested, and, as a practical matter, Plaintiffs' counsel recognize that taking such large numbers to a jury presents substantial strategic risks. *Id.* Even a number in the mid-hundreds of millions potentially risks offending a jury, and leading to a nominal award – or no monetary award at all.

The Out-of-Pocket Consequential Damages theory, which is more tangible, applies to only a relatively small subset of the class, and would have required class members to come forward individually and document their losses with respect to a breach that happened years before trial. *See* Class Cert. at 22-23; Order on 2nd MTD at 22-29. Anthem also had presented evidence

raising doubts about Plaintiffs' ability to pinpoint the source of any identity fraud, having forensically examined Plaintiffs' computers to test for the possibility that malicious software compromised their personal information, catalogued other data breaches that involved Plaintiffs' data, and retained an expert to attempt to demonstrate that Plaintiffs' private information being offered for sale on the Dark Web was unrelated to the Anthem data breach. Class Cert. Opp. at 21-23.

2. The Risk, Expense, Complexity, and Likely Duration of Further Litigation

Overall, it is fair to characterize this litigation as a strong data breach case, but a very complex one that still faces numerous hurdles, a well-funded and committed defense, and a wide range of possible outcomes. The case involves millions of people, hundreds of legal claims that implicate several different legal doctrines and the laws of all fifty states, highly technical subject matter, ten expert witnesses, and a pending class certification motion and related *Daubert* motions. Plaintiffs have spent close to $2 million on the litigation to date, and those expenses would only continue to mount if the litigation were to continue. Cervantez Decl. ¶ 56.

Almost all class actions involve a high level of risk, expense, and complexity, which is one reason that judicial policy so strongly favors resolving class actions through settlement. *Linney v. Cellular Alaska P'ship*, 151 F.3d 1234, 1238 (9th Cir. 1998). But this is an especially complex class proceeding in an especially risky field of litigation. Historically, data breach cases faced substantial hurdles in making it past the pleading stage. *See Hammond v. The Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, at *1 (S.D.N.Y. June 25, 2010) (collecting cases and noting that "every court to [analyze data breach cases] has ultimately dismissed under Rule 12(b)(6) … or under Rule 56 following the submission of a motion for summary judgment); *In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, 2010 WL 3341200, at *6 (W.D. Ky. Aug. 23, 2010) (approving data breach settlement, in part, because "proceeding through the litigation process in this case is unlikely to produce the plaintiffs' desired results"). The law has gradually adapted to this relatively new type of litigation, and through cases like this one, precedent has been mounting for holding corporations responsible when they collect private data without adequately securing it. But the path to a class-wide monetary judgment remains untrodden, and it will take some time

before litigants and courts navigate all the unique issues posed by data breach lawsuits and some level of certainty sets in – particularly in the area of damages. For now, data breach cases are among the most risky and uncertain of all class action litigation, making settlement the more prudent course when a reasonable deal is on the table.

By settling now, class members can obtain timely and practical remedies that otherwise would not be available for years, if at all. What typical class members want most is not their share of a hypothetical billion-dollar judgment (which would amount to about $13 per class member), but for their private information to remain confidential and secure. Extended credit monitoring services and immediate changes to Anthem's data-security practices can help achieve that goal. Credit monitoring works to prevent and detect misuse of information taken in the data breach, while changes in data-security practices work to reduce the risk of future breaches. Plaintiffs had requested both as equitable relief, but by the time that Plaintiffs obtained a judgment and Anthem had exhausted its appeals, neither would be of as much value to class members. Credit monitoring services are needed most in the first four to five years after a data breach occurs, and security measures are most effective the sooner they can be implemented. *See* Class Cert. at 13; Cervantez Decl. ¶ 14. This is a case, in other words, where delay hurts class members, making prompt settlement all the more important. Absent a settlement, there is nothing class members can individually do to make the personal information stored in Anthem's data warehouse more secure, and the only way that they could obtain credit monitoring is to purchase it themselves – at the high retail cost of $9-$20 per month (which they may not be able to afford). Cervantez Decl. ¶ 15.

3. <u>The Risk of Maintaining Class Action Status Through Trial</u>

None of the hundreds of claims involved in this litigation have been certified yet. Plaintiffs have filed a motion to certify four bellwether claims, and Anthem has opposed, with the two sides submitting hundreds of exhibits and reports from ten expert witnesses. *See* Plaintiffs' Revised Index of Evidence [ECF 752]; Defendants' Index of Evidence [ECF 805-1]. While Plaintiffs believe they have made a strong showing on the four bellwether claims, as with other aspects of data breach litigation, there is little directly analogous precedent to rely upon. Class certification has been denied in other consumer data breach cases. *See* Class Cert. Opp. at 21. Indeed, it was

only earlier this year that the first litigation class was certified in a consumer data breach case. *See Smith v. Triad of Alabama, LLC*, 2017 WL 1044692, at *16 (M.D. Ala. Mar. 17, 2017). Plaintiffs expect that there should and will be more data breach certifications to come, and see no reason why Plaintiffs' claims should be treated differently than the contract and consumer protection claims that are regularly certified in non-data breach cases. But the dearth of direct precedent adds to the risks posed by continued litigation.

4. The Amount Offered In Settlement

In light of the risks and uncertainties presented by data breach litigation, the $115 million settlement fund achieved for the class in this case is truly groundbreaking. An insurance company that specializes in data breaches, and publishes a regular newsletter on data breach legal issues and trends, wrote last year: "[D]efendants are unlikely to pay *anywhere close* to $1 per class member to settle an action brought by a class on behalf of 100 million potentially affected individuals." Marcello Antonucci et al., *Post-Spokeo, Data Breach Defendants Can't Get Spooked – They Should Stand Up To The Class Action Plaintiff Bogeyman*, Beazley Breach Insights, Oct. 27. 2016, https://www.beazley.com/documents/Insights/201610-data-breach-class-action-settlements.pdf (emphasis added). While reducing the settlement achieved here to what the Company will pay out-of-pocket per class member ignores the comprehensive, and costly, business practice changes to improve its data security and the true value of the settlement to the Class, here, Defendants have agreed to pay $1.46 per class member – by far the highest figure any defendant has ever paid as the result of a large data breach affecting millions of consumers. By way of example:

- The Home Depot data breach, which involved the theft of approximately 40 million consumers' payment data and 53 million consumers' email addresses, resolved with Home Depot creating a $13 million fund for consumers, paying an additional $6.5 million for internet and dark web monitoring services (which was eligible to be repaid from the fund), paying the costs of notice and settlement administration (which also were eligible to be repaid from the fund), and paying $7.5 million in attorney fees. *See In re the Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-02583-

TWT, ECF 181-2 (March 7, 2016) (Settlement Agreement); *id.*, 2016 WL 6902351, at *6 (N.D. Ga. Aug. 23, 2016) (order approving settlement).

- The Target data breach, which compromised the personal information of nearly 100 million consumers, resolved with Target establishing a settlement fund of $10 million, paying the costs of notice and settlement administration, and paying $6.75 million in attorney fees. *See In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-MD-2522-PAM, ECF 358-1 (March 18, 2015) (Settlement Agreement); *id.*, 2017 WL 2178306, at *2 (D. Minn. May 17, 2017) (order approving settlement on remand from the 8th Circuit).
- The Ashley Madison data breach, which exposed the personal information of 36 million customers and has been linked to divorce proceedings, blackmail attempts, and at least two suicides, recently resolved with Ashley Madison agreeing to establish a settlement fund of $11.2 million. *See In re Ashley Madison Customer Data Security Breach Litigation*, No. 4:15-MD-02669-JAR, ECF 354, at *5-6 (E.D. Mo. July 21, 2017) (preliminary approval order).

These comparisons are not intended to disparage the settlements achieved in those cases, but to underscore that Plaintiffs have capitalized on the strength of their case and achieved good value for the class. The benefits offered to class members are particularly timely as well, coming soon after the two years of credit monitoring initially offered by Anthem has expired. Class members will receive a minimum of two additional years of credit monitoring, with a possibility that the credit monitoring will be extended for an additional two years if funds remain in the Settlement Fund after other distributions, such that the Settlement may meet or exceed the five years of credit monitoring recommended by Plaintiffs' expert. *See* SA ¶ 7.1. And for those class members who have already purchased credit monitoring for themselves, or otherwise incurred expenses as a result of the data breach, they will now be able to recover those expenses – and they will be able to do so using a relaxed causation standard. *See id.* ¶¶ 1.23, 6.3. The proposed settlement will also allow all class members – even those who fail to enroll in the monitoring

services – to seek assistance with fraud resolution if they should fall victim to identity theft during the period while credit monitoring services are in effect. *Id.* ¶ 4.9.

While the size of the Settlement Fund is indeed groundbreaking, $115 million understates the value of the Settlement to class members. Because the Settlement Fund will be used to purchase credit monitoring in bulk, the Settlement generates economies of scale that would not otherwise be available to individual class members. If this case did not settle and class members wanted to purchase comparable credit monitoring services from Experian themselves, they would need to spend between $9.99 and $19.99 per month. Cervantez Decl. ¶¶ 9, 15. The credit monitoring alone can thus be valued at more than $240 per class member – or even more than $480 per class member if sufficient funds remain to extend the credit monitoring for an additional 24 months. When multiplied by the 891,431 class members who have filed claims for credit monitoring so far, that yields a value of between $213 and $427 million. And when multiplied by all 80 million members of the class, the retail value of credit monitoring services made available to the class reaches into the billions. *See Johansson-Dohrmann v. Cbr. Sys., Inc.*, 2013 WL 3864341, *5, 9 (S.D. Cal. July 24, 2013) (valuing settlement using retail value of credit monitoring services made available to the class).

The settlement also has added value to class members going forward, in that it will reduce the risk that the private information class members have entrusted to Anthem – and continue to entrust to Anthem – is compromised by future attacks. Settlement Ex. 2 [ECF 869-11]. While Plaintiffs have not attempted to put a monetary value on the significant business practice commitments that Anthem has made under the Settlement, at a minimum, Anthem will be required to spend [redacted] over the next three years to help protect class members' personal information – [redacted] more than it would have spent if Anthem's data-security budget remained at pre-breach levels. *Id.* ¶ 8. When combined with the $115 million settlement fund, the two years of credit monitoring that Anthem purchased for class members during the litigation, and the outlays Anthem has already made to upgrade its security during the litigation, Plaintiffs are confident that this litigation has created strong incentives not only for Anthem, but for the many

other companies who collect vast amounts of the public's private information, to invest in appropriate levels of data security.

5. The Extent of Discovery Completed and The Stage of Proceedings

Before entering into settlement discussions on behalf of class members, counsel should have "sufficient information to make an informed decision." *Linney*, 151 F.3d at 1239. In the two years after Plaintiffs' counsel filed the consolidated class complaint, they have litigated two motions to dismiss, 14 discovery motions before this Court and one in Washington, D.C. to compel production of federal government documents; reviewed 3.8 million pages of documents; deposed 18 percipient fact witnesses, 62 corporate designees, and six defense experts; produced reports from four experts and defended their depositions; produced over 100 plaintiffs for depositions and produced 29 of those plaintiffs' computers for forensic examinations; and fully briefed class certification and related *Daubert* motions. Cervantez Decl. ¶ 3. They know the strengths and weaknesses of the class's claims, have worked extensively with experts to value those claims and to understand the business practice changes necessary to protect class members' data in the future, and are well-equipped to negotiate a settlement on behalf of the class. *Id.* ¶ 19.

6. The Experience and Views of Counsel

The Court appointed experienced and qualified counsel with substantial experience litigating complex class actions of all kinds, including data breach cases, to serve as Plaintiffs' Lead Counsel and Steering Committee. *See* 9/11/15 Order [ECF 284]; ECF 751-14 to 761-17. Those attorneys have represented Plaintiffs and putative class members in that role for more than two years, devoting tens of thousands of hours to the case, and have no reservations in recommending the Settlement as a very good deal for the class. Cervantez Decl. ¶ 20; Friedman Decl. ¶ 2, Sobol Decl. ¶ 23, Gibbs Decl. ¶ 2.

7. The Presence of a Government Participant

No governmental agency is involved in this litigation, but the Attorney General of the United States and Attorneys General of each of the States have been notified of the proposed settlement pursuant to the Class Action Fairness Act, 28 U.S.C. § 1715, and given an opportunity

to raise any objections or concerns they might have. *See* Geraci Decl. ¶¶ 2-3. To date, none of these government officials have come forward with any complaints about the Settlement. *Id.* ¶ 5.

It is also worth noting that eight state insurance commissioners entered into a separate settlement with Anthem in December 2016. That settlement is far less expansive than the proposed settlement now before the Court. It only provided additional credit protection for affected minors (at an estimated cost of $15 million), and required that Anthem finish implementing security measures that it was already in the process of installing (at an estimated cost of $30 million). Cervantez Decl. Ex. 14, Sec. D. Although the insurance commissioners are empowered to assess administrative fines and penalties, they specifically found that no additional relief was warranted and that Anthem's pre-breach cybersecurity was reasonable. *Id.*, Sec. A.5(a), A.7.

8. The Reaction of Class Members to the Settlement

Class Members have until December 29, 2017 to comment on the Settlement, so it is not yet possible to fully assess this factor. 8/25/17 Order ¶¶ 14-16. Early returns are promising, however. The Settlement is receiving a high level of interest from class members, with 855,767 people visiting the Settlement Website to date and 82,020 people calling the Settlement Administrator's automated phone line for more information. Geraci Decl. ¶¶ 19-20. The Settlement has also received a fair amount of national media attention, with NBC News, USA Today, and CNET, among others, reporting on the remedies available to class members. *See, e.g.*, https://www.nbcnews.com/news/us-news/anthem-pay-record-115m-settle-lawsuits-over-data-breach-n776246; https://www.usatoday.com/story/money/business/2017/06/26/anthem-settles-security-breach-lawsuit-affecting-80m/103217152; https://www.cnet.com/news/anthem-would-pay-record-115m-to-settle-data-breach-suit.

Class members will have until January 29, 2018 to file claims for credit monitoring or alternative compensation and another year to claim out of pocket damages. But already, 891,431 class members have filed claims for credit monitoring, 106,417 class members have filed claims for alternate compensation, and 11,680 class members have filed claims for out-of-pocket costs. Geraci Decl. ¶¶ 21-22. In contrast, only eight class members have objected to or commented on

the settlement and only 169 have submitted opt-out requests. ECF Nos. 906-908, 911-913; Geraci Decl. ¶¶ 23-24. To avoid duplicative briefing and conserve judicial resources, Plaintiffs will wait until the objection deadline has passed, and address all objections lodged by the class together in their reply brief. At this point, however, it is fair to say that the class's level of participation reflects well on the settlement and indicates that it is providing needed relief.

9. Lack of Collusion Among the Parties

When a proposed settlement is negotiated prior to class certification, the Ninth Circuit has emphasized that "consideration of th[e] eight *Churchill* factors alone is not enough to survive appellate review," and that the district court should also scrutinize the settlement for subtle signs of collusion or conflicts of interest. *In re Bluetooth*, 654 F.3d at 946. Signs that the Ninth Circuit has said may indicate that plaintiffs' counsel may have allowed pursuit of their own self-interests to infect negotiations include:

(1) when counsel receive a disproportionate distribution of the settlement, or when the class receives no monetary distribution but class counsel are amply rewarded

(2) when the parties negotiate a "clear sailing" arrangement providing for the payment of attorneys' fees separate and apart from class funds

(3) when the parties arrange for fees not awarded to revert to defendants rather than be added to the class fund

Id. at 947 (internal quotation marks omitted). None of those warning signs are present here. Class Counsel will not receive a disproportionate distribution of the settlement. As explained in Plaintiffs' fee application, Class Counsel is requesting attorneys' fees that fall well within the range of permissible percentage-based awards and reflect a negligible multiplier, if any. The parties also did not negotiate a clear sailing arrangement that provides for the payment of fees separate from class funds. Class Counsel's fees will be paid from the same non-reversionary Settlement Fund as class members, and so Class Counsel had every reason to negotiate the largest fund possible. And rather than revert to Defendants, any fees that are not awarded to Class Counsel will remain in the Settlement Fund. Finally, it bears mentioning that the settlement was negotiated over the course of several full-day mediation sessions with Judge Layn R. Phillips (Ret.), and the final terms stemmed from Judge Phillips' mediator's proposal. *See G. F. v. Contra*

Costa Cty., 2015 WL 4606078, at *13 (N.D. Cal. July 30, 2015) ("[T]he assistance of an experienced mediator in the settlement process confirms that the settlement is non-collusive.") (internal quotation marks omitted).

IV. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court approve the parties' settlement and enter judgment consistent with its terms.

Respectfully Submitted,

ALTSHULER BERZON LLP
EVE H. CERVANTEZ
JONATHAN WEISSGLASS
DANIELLE LEONARD
MEREDITH JOHNSON
TONY LOPRESTI

Dated: December 1, 2017

By: /s/ *Eve H. Cervantez*
Eve H. Cervantez

COHEN MILSTEIN SELLERS & TOLL PLLC
ANDREW N. FRIEDMAN
GEOFFREY GRABER
SALLY M. HANDMAKER
ERIC KAFKA

Dated: December 1, 2017

By: */s/ Andrew N. Friedman*
Andrew N. Friedman

Lead Plaintiffs' Counsel

LIEFF CABASER HEIMANN & BERNSTEIN, LLP
MICHAEL SOBOL
JASON LICHTMAN

GIRARD GIBBS LLP
ERIC GIBBS
DAVID BERGER

Plaintiffs' Steering Committee