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 PRELIMINARY APPROVAL OF CLASS ACTION SETTLEMENT** Date: August 17, 2017 Time: 1:30 p.m. Judge: Hon. Lucy H. Koh Crtrm: 8, 8th Floor

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

I. INTRODUCTION

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 has denied that the stolen information has ever been misused.

After two years of litigation that included two motions to dismiss, over two hundred depositions, ten expert witnesses, full briefing on class certification, and three days of mediation, the parties accepted a mediator's proposal that—if approved by the Court—would result in the largest data breach settlement in history. The proposed settlement requires Anthem to establish a $115-million non-reversionary settlement fund for the benefit of the class. The fund will be used to purchase at least two years of credit monitoring services for class members, which will help protect them from fraud and ensure that any identity theft is detected and remedied quickly. Were class members to purchase these credit monitoring services themselves, they would have to pay between $9 and $20 per month, but the parties can obtain them for a fraction of that cost by purchasing them in bulk. The fund will also be used to individually notify class members about the settlement, to encourage class members to sign up for credit monitoring, and to explain that *all* class members will remain eligible for fraud-resolution services for at least two years, even if they choose to forego credit monitoring. In addition, $15 million of the fund will be set aside to pay out-of-pocket expenses incurred as a result of the data breach. For those class members who already have their own credit monitoring service and do not wish to enroll in the service provided by the settlement, the Settlement provides for alternative compensation, as much as $50 per class member.

The proposed settlement also requires Anthem to spend at least [redacted] to help protect class members' personal information over the next three years. Anthem will additionally be required to implement or maintain meaningful, specific changes to its data security practices that directly address the security elements that Plaintiffs believe contributed to the breach.

Plaintiffs believe that the proposed settlement is a favorable one for the class and seek

preliminary approval of the settlement. Declaration of Eve Cervantez ("Cervantez Decl.") at ¶ 9. By settling now, the class is able to take advantage of remedies that, as a practical matter, would be unavailable or worth substantially less by the time this case could be litigated to a final judgment. *Id*. Plaintiffs believe that credit monitoring services are most critical in the first five years after a data breach, and the two years of free credit monitoring provided by Anthem have recently expired. *Id.* Similarly, changes to Anthem's data security practices will be most effective the sooner they are implemented. *Id.* By providing class members with extended credit monitoring and requiring enhanced data security *now*, the proposed settlement helps preserve the confidentiality of class members' private information in ways that a later monetary judgment could not. *Id*. Accordingly, Plaintiffs respectfully request that the Court preliminarily approve the parties' Settlement Agreement – attached as Exhibit A to the accompanying Declaration of Eve H. Cervantez and cited hereafter as "SA" or "Settlement" – and enter an order that:

1. Certifies the proposed settlement class under Rule 23(b)(3);
2. Preliminarily approves the proposed settlement as fair, reasonable, and adequate;
3. Directs notice to be disseminated to class members in the form and manner proposed by the parties as set forth in the Settlement and Exhibits 4-7 thereto;
4. Appoints KCC to serve as the Settlement Administrator; and
5. Sets a hearing date and schedule for final approval of the settlement and consideration of Class Counsel's fee application.

II. BACKGROUND

A. Plaintiffs' Claims

After Anthem announced the data breach in early 2015, 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 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 depends, above all, on proving their allegations that the data breach was possible only because Anthem had aggregated 80 million people's private information into a central data warehouse that was not properly

secured. On behalf of those individuals, Plaintiffs have 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 an expert report 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. ¶ 7.

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 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 recently expired for most of the class, however, and because Plaintiffs believe it is important to protect against identity theft or other forms of impersonation in 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 wanted that credit monitoring to be more extensive than the AllClear services offered by Anthem, which, for example, only monitored one of the three major credit bureaus for potential fraudulent activity. Van Dyke Report ¶ 50(b); *see also* Cervantez Decl. ¶ 7.

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 cyber security of personal information. *See* LoPresti Decl. in

Support of Class Cert [ECF No. 749-1] ¶ 3. For settlement purposes only, Plaintiffs determined that this change sufficiently addressed their concerns. Cervantez Decl. ¶ 8.

2. Monetary Remedies

Plaintiffs requested monetary relief in the Complaint under three theories: Benefit of the Bargain, Loss of Value of PII, and Consequential Out-of-Pocket Expenses. *See* 2nd MTD Order [ECF 524] at 22-29. The Benefit of the Bargain theory would compensate class members based on the difference in value between the health insurance Anthem provided (which Plaintiffs allege lacked adequate data security) and the value of the health insurance that Anthem should have provided (which would have included 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]. Because the parameters of the conjoint surveys would depend on the classes ultimately certified by the Court, Plaintiffs' expert had not completed his conjoint analysis prior to settlement. *See* Cervantez Decl. ¶ 8.

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 certain types of PII fetch 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 protecting 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 money spent to rectify identity fraud, including delayed tax refunds, 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, a few

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 five 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 Court further streamlined the bellwether process by ordering that Plaintiffs move for class certification on only four claims: California and federal breach of contract and California and New York consumer protection. ECF 601 at 1. 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 105 plaintiffs and four expert witnesses for deposition (with 29 of the plaintiffs also producing their computers for forensic imaging); and exchanged interrogatories, RFAs, and expert reports with Defendants. Cervantez Decl. ¶ 2. 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.* ¶ 3.

While the parties were briefing class certification, they were also engaging in a series of mediation sessions with Judge Layn R. Phillips (Ret.). *Id.* ¶ 6. 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. Terms 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.

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, but 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] to information security. It will now be required to spend at least [redacted] over the next three years—a figure that represents a three-fold increase over Anthem's pre-breach allocation. SA Ex. 2 ¶ 8. Anthem will also be required to make or maintain over the next three years a number of specific changes to the manner in which it secures class members' personal information. *See* Settlement Ex 2. These measures were derived in consultation with security professionals based on Plaintiffs' extensive discovery, and squarely address the five categories that Plaintiffs had focused on in the litigation (*see* Class Cert. at 3-4):

(i) Failure to require [redacted]: Anthem expanded its implementation of [redacted] after the breach. It will be required to maintain that [redacted], and additionally will be required to ensure through [redacted] when accessing Anthem's network. SA Ex. 2 ¶ 5.

(ii) Failure to [redacted] Enterprise Data Warehouse: Anthem will be required to maintain its recently implemented [redacted] for its database environments that use [redacted] to flag suspicious events. *Id.* ¶ 13.

(iii) Failure to monitor suspicious network activity: Anthem has increased the network logs it generates by five-fold and is now required to monitor its logs by feeding them into software tools. *Id.* ¶ 6.

(iv) Failure to [redacted]: Anthem's [redacted] are now stored in [redacted] *Id.* ¶ 13.

(v) Failure to [redacted] data stored on the Enterprise Data Warehouse: [redacted] Enterprise Data Warehouse will be [redacted], with other [redacted] to be [redacted]. *Id.* ¶ 3.

Plaintiffs also alleged that Anthem's failure to remove old member data from the Enterprise Data Warehouse was a factor that exacerbated the scope of the data breach, which included [redacted]. Class Cert. at 2. Under the settlement, Anthem will be required to retain no more than the latest [redacted] in the Enterprise Data Warehouse; to archive older data in a separate database that will be subject to enhanced access controls; and to permanently delete data that no longer needs to be retained on an annual basis. SA Ex. 2 ¶¶ 1-2.

To ensure that Anthem maintains enhanced security measures, and that those 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 & Ex. 2 ¶ 7. Anthem will also conduct adversarial simulations at least twice a year, which will mimic a malicious attacker with internal access to Anthem's network. SA Ex. 2 ¶ 10. 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. *Id.* ¶¶ 9 & 11.

These immediate fortifications to Anthem's systems represent significant improvements in Anthem's security practices, and move substantially towards closing 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. Further, the cost and public nature of this litigation, including this Court's rulings, serve as long term incentives for Anthem to deploy appropriate data security, and also serve as a deterrent to regressing to past practices.

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 into a Qualified Settlement Fund. SA ¶ 3.1. From the net settlement fund, $15 million will be set aside to reimburse Settlement Class Members who had verifiable out-of-pocket losses, and the rest will be distributed equally to Settlement Class Members who choose between Credit Monitoring Services or cash (if they already have Credit Monitoring Services) as follows. *Id.* ¶¶ 5.3 & 6.4.

a.) Fraud Protection and Credit Monitoring. Settlement funds will first be used to provide class members with two years of identity fraud prevention and detection services from Experian, including:

- Daily credit monitoring at all three major credit reporting agencies;
- An Experian (1B) Credit Report upon enrollment;
- Experian Credit Reports;
- ID Theft Insurance, which covers certain identity theft related expenses up to a limit of $1 million;
- "Dark Web" monitoring for personal information;
- Identity Validation monitoring and alerts;
- Fraud Resolution Services that provide professional fraud resolution assistance to Settlement Class Members who experience identity theft or fraud, helping them with identity recovery and restoration.

Id. ¶ 4.1. Class members will receive protections beyond what Anthem had offered them through AllClear – including triple-bureau monitoring – and those protections will extend the total duration of fraud detection services offered to class members to at least four years, perhaps more.

Class members will be encouraged to sign up for these credit services, regardless of whether they previously signed up for AllClear credit monitoring, and will be able to claim services easily: either by filling out and returning the tear-off portion of the postage-prepaid postcard notice they will receive from the Settlement Administrator, by visiting the Settlement Website and completing an online claim form, or by calling the telephone number listed on the postcard notice. *Id.* ¶ 4.3 & Exs. 5(a), 7. Class members will be encouraged to sign up for credit monitoring, and educated about the benefits of doing so. SA ¶ 4.5 & Exs. 4, 5. Significantly, even if Settlement Class Members choose to forego credit monitoring for now, if they 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, without ever filing a claim form. *Id.* ¶ 4.9.

b.) Alternative Compensation. Class members who already have credit monitoring services can instead select alternative cash compensation. *Id.* ¶ 5.1. Class members will receive up to a maximum of $50. *Id.* ¶ 5.3. As an initial matter, the Net Settlement Fund (after paying all other claims, fees, and expenses) will be used to distribute up to $36 to each Settlement Class Member (to be reduced *pro rata* if necessary). *Id.* ¶ 5.3. If, however, the aggregate amount of all claims for Alternative Compensation is less than $13 million, then the amount distributed will be increased *pro rata*, to a maximum amount of $50 per Settlement Class Member. *Id.* To request the Alternative Compensation, class members will simply need to confirm the timing and type of credit monitoring services they already have and that they wish to receive the alternative compensation instead through the on-line claims process. *Id.* ¶ 5.2; Settlement Ex. 7.

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 connected to the data breach. *Id.* ¶ 6.4. Reimbursable expenses may include unreimbursed claimed fraud losses or charges; time spent remedying issues related to the breach, at $15 per hour or unpaid time off work, whichever is greater; professional fees incurred in connection with identity theft or falsified tax returns; credit freezes; credit monitoring ordered between January

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; Settlement Ex. 6. So long as the claimed fraud is fairly traceable to the Anthem Data Breach – meaning it involved possible mis-use 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. Claims can be submitted for up to a year after Final Approval or until the $15 million allocated for out-of-pocket reimbursements is exhausted, whichever occurs first. *Id.* ¶¶ 6.1 & 6.4. Plaintiffs expect that $15 million allocated will be more than enough to accommodate all out-of-pocket claims, but if those funds are exhausted, class members will be so informed through the Settlement Website. *Id.* ¶ 6.4; Cervantez Decl. ¶ 12. The Settlement Administrator will review claims as they are submitted and will have authority to determine whether and to what extent a claim for out-of-pocket costs is valid. SA ¶ 6.2.

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 the credit monitoring services offered by the Settlement, Plaintiffs expect the costs of notice and settlement administration to be substantial—approximately $23 million (with a large percentage of this amount to cover the cost of postage on a postcard notice that will allow tear-off and return claims for credit monitoring services). Cervantez Decl. ¶ 16. The parties have retained KCC to serve as the Settlement Administrator, subject to Court approval.

Notice will be mailed to approximately 50 million class members for whom addresses are available, via a double-postcard with a detachable claim form that includes business return mail postage. SA Ex. 4 at 13. Additionally, email notification will be sent to the approximately five million class members for whom email addresses are available. *Id.*. Notice will also be published

in *People* and *Good Housekeeping*. *Id.* at 14. Significantly, in addition to these traditional forms of notice, the parties have agreed to an additional innovative notice plan using internet media ads, which will involve 180 million impressions distributed over Google Display Network and social media sites (Facebook, Instagram, LinkedIn, and Twitter) on mobile and desktop devices. *Id.* at 15-16. The digital media campaign will be actively monitored to continuously post on sites that have proven successful at reaching class members throughout the course of the campaign. *Id.* The point of the internet campaign is not only to reach class members for whom the parties lack addresses, but also to encourage class members who received postcard notice to file a claim for credit monitoring services (or cash) and out of pocket expenses incurred. Cervantez Decl. ¶ 17.

e) Service Awards to Named Plaintiffs. Plaintiffs will separately petition the Court to award each named plaintiff up to $7,500 (for those whose computers were forensically imaged) and $5,000 (for all other named plaintiffs) from the Settlement Fund in recognition of the time, effort, and expense they incurred pursuing claims against Defendants that ultimately benefited the entire class. Defendants have agreed not to oppose any such application.

f) Attorney Fees and Costs. Plaintiffs will also separately petition for an award of attorneys' fees and reimbursement of litigation expenses from the Settlement Fund. Plaintiffs will not seek more than 33% of the Settlement Fund ($37,950,000) for attorney fees, which as counsel pledged at the onset of the litigation will amount to considerably less than 1.75 times their reasonable lodestar, already reduced in the exercise of billing judgment. Cervantez Decl. ¶ 18. They will also will not seek more than $3,000,000 in expense reimbursements, and will support their application with detailed lodestar information and an accounting of their expenses. *Id.* ¶ 19. Defendants have agreed not to oppose Plaintiffs' application.

g) 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 extend credit monitoring for at least one month, or if there are funds remaining after credit monitoring is extended, the remainder will be distributed *cy pres* to the Center for Education and

Research in Information Assurance Security at Purdue University and the Electronic Frontier Foundation. SA ¶ 7.1. The Center for Education and Research in Information Assurance Security at Purdue University is a national center for research and education in areas of information security. The Electronic Frontier Foundation is a nonprofit organization that champions user privacy and technology development. 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.

III. ARGUMENT

A. The Proposed Settlement Class Should Be Certified

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

Before assessing the parties' settlement, the Court should first confirm that the underlying settlement class meets the requirements of Rule 23. *See Amchem Prods. v. Windsor*, 521 U.S. 591, 620 (1997); Manual for Complex Litigation, § 21.632. 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 78.8 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 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

[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, PACER Dkt. No. 3230 at 5-6 (N.D. Cal. May 17, 2017).

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 here. 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 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. The Class Meets The Requirements Of Rule 23(b)(3)

"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*, 521 U.S. at 620. 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 Proposed Settlement Should Be Preliminarily Approved

Before the parties' settlement can be approved, the class members who will be bound by its terms must be notified and given an opportunity to object or otherwise react to the proposed settlement. Fed. R. Civ. P. 23(e). This notification process takes time and can be quite expensive, so it has become customary for courts to first conduct a preliminary fairness review. *See* Newberg on Class Actions § 13:10 (5th ed.). There is "relatively scant appellate authority regarding the standard that a district court must apply in reviewing a settlement at the preliminary approval stage." *In re High-Tech Employee Antitrust Litig.*, 2014 WL 3917126, at *3 (N.D. Cal. Aug. 8, 2014). In the past, courts have focused only on whether the proposed agreement appears to be non-collusive, is free of "obvious deficiencies," and generally falls within the range of "possible" approval. *See, e.g., In re Tableware Antitrust Litig.*, 484 F. Supp. 2d 1078, 1079-80 (N.D. Cal. 2007). More recently, however, several courts in this district have criticized the notion that review

of proposed class settlements at the preliminary approval stage need only involve a "quick look," or a watered-down version of final approval. *See Cotter v. Lyft, Inc.*, 193 F. Supp. 3d 1030, 1036 (N.D. Cal. 2016); *O'Connor v. Uber Techs., Inc.*, 201 F. Supp. 3d 1110, 1122 (N.D. Cal. 2016); *Viceral v. Mistras Grp., Inc.*, 2016 WL 5907869, at *6 (N.D. Cal. Oct. 11, 2016).

Plaintiffs agree that a reduced level of scrutiny at the preliminary approval stage "makes little practical sense, from anyone's standpoint," and undercuts the "more exacting review" that must ultimately be applied to class settlements reached prior to certification. *Cotter*, 193 F. Supp. 3d at 1036; *Lane v. Facebook, Inc.*, 696 F.3d 811, 819 (9th Cir. 2012).

Accordingly, Plaintiffs address each of the following settlement factors articulated by the Ninth Circuit (while recognizing that at least one of those factors—the reaction of class members—is not yet known) and submit that they collectively weigh in favor of judicial approval:

(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).

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, Plaintiffs submit that 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 alike. *Id.* Plaintiffs believe they had 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. ¶ 11. 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 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 over $2 million on the litigation to date, and those expenses would only continue to mount if the litigation were to continue. Cervantez Decl. ¶ 19.

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, practical remedies also become available to class members that will soon disappear. 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 Dec. ¶ 9. This is a case, in other words, where delay hurts class members. There is nothing they 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). *Id.*

3. The Risk of Maintaining Class Action Status Through Trial

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 No. 752]; Defendants' Index of Evidence [ECF No. 805-1]. But 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 a few months ago that the first litigation class was certified in a consumer data breach case. *See Smith v. Triad of Alabama, LLC*, 2017 WL 1044692, at *6 (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). Yet, in this case, 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, and has also agreed to comprehensive, and costly, business practice changes to improve its data security. Likewise, the overall settlement fund far exceeds what has been paid in data breach settlements to date. 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), and $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 No. 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 and separately paying $6.75 million in attorney fees. *See In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL 14-2522-PAM, ECF No. 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)

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 right as the two years of credit monitoring initially offered by Anthem is expiring. By acting now, the class can use the settlement fund to purchase credit monitoring services in bulk at a fraction of the services' retail cost. *See* SA ¶ 4.6; Cervantez Decl. ¶ 9. In this way, the proposed settlement is able to offer 78.8 million class members the opportunity to receive – for free – what they would otherwise cost them $9-20 per month in the retail market. *See* Class Cert at 13. 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 amount 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.

The proposed settlement will also reduce the risk that the private information class members have entrusted to Anthem – and continue to entrust to Anthem – is compromised by future attacks. SA Ex. 2. 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 twenty months since Plaintiffs' counsel filed the consolidated class complaint, they have litigated two motions to dismiss, 14 discovery motions before this Court and one in 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 five defense experts; produced reports from four experts and defended their depositions; produced 105 plaintiffs for depositions and produced 29 of those plaintiffs' computers for forensic examinations; and fully briefed class certification and related *Daubert* motions. Cervantez Decl., ¶ 2. 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.* ¶ 3.

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 Nos. 751-14 to 761-17. Those attorneys have represented Plaintiffs and putative class members in that role for nearly

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., ¶ 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 will be 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 may have.

8. The Reaction of Class Members to the Proposed Settlement

The class has yet to be notified of the settlement and given an opportunity to object, so it is premature to assess this factor. Before the final approval hearing, the Court will receive and have a chance to review all objections or other comments received from class members, along with a full accounting of all opt-out requests.

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. Plaintiffs' counsel will be paid from the same non-reversionary Settlement Fund as class members, and so had every reason to negotiate the largest fund possible. Plaintiffs'

counsel promised at the outset of this litigation that they would not request fees amounting to any more than 1.75 times their lodestar, and while their obligations are far from finished, they intend to request a multiplier substantially below 1.75. Cervantez Decl. ¶ 18. Plaintiffs' fee request will also constitute no more than 33% of the Settlement Fund, which is within the range of permissible percentage-based awards—particularly considering the additional value provided by the settlement's non-monetary relief and the relatively modest multiplier. Of course, the Court will have ultimate discretion over how much of the Settlement Fund should go toward fees after reviewing counsel's detailed lodestar data and considering all applicable factors. 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)).

C. The Proposed Notice Plan Should Be Approved

1. The Settlement Provides for the Best Method of Notice Practicable Under the Circumstances.

The federal rules require that before finally approving a class settlement, "[t]he court must direct notice in a reasonable manner to all class members who would be bound by the proposal." FRCP 23(e)(1). Where the settlement class is certified pursuant to Rule 23(b)(3), the notice must also be the "best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort." FRCP 23(c)(2)(B).

The parties have agreed on a notice plan that would provide class members with direct mail notice and direct email notice to the extent that mail and email addresses are available, publication notice in two popular magazines, and an innovative social media campaign designed to both reach more class members, and encourage them to claim services under the Settlement. Plaintiffs request that the Court approve this method of notice as the best practicable under the circumstances.

2. The Proposed Form Of Notice Adequately Informs Class Members Of The Settlement And Their Right To Object.

The notice provided to class members should "clearly and concisely state in plain, easily understood language" the nature of the action; the class definition; the class claims, issues, or defenses; that the class member may appear through counsel; that the court will exclude from the class any member who requests exclusion; the time and manner for requesting exclusion; and the binding effect of a class judgment on class members. Fed. R. Civ. P. 23(c)(2)(B). The form of notice proposed by the parties complies with those requirements. Class members will receive a postcard in the mail designed to catch their attention and alert them to the settlement and available remedies. *See* SA, Ex. 5(a). It will also direct them to the Settlement Website, where more information—including a detailed long-form notice and other case documents including the operative consolidated class action complaint and Settlement Agreement—will be made available. *See id.*, Ex. 5(b). Plaintiffs believe that this is the most effective way to alert class members to the existence of the settlement and convey detailed information about the settlement approval process, and accordingly ask that the Court approve the proposed forms of notice. Cervantez Decl. ¶ 16; *see Schaffer v. Litton Loan Servicing, LP*, 2012 WL 10274679, at *8 (C.D. Cal. Nov. 13, 2012) (approving similar postcard notice plan). Class members will also be alerted to the Settlement by publication in two popular magazines and an internet advertising campaign. SA Exs. 4, 5(d).

3. Notice of the Settlement Will Be Provided to Appropriate Federal and State Officials.

Anthem will provide notice of the proposed settlement to the U.S. Attorney General and appropriate regulatory officials in all 50 states, as required by the Class Action Fairness Act, 28 U.S.C. § 1715. SA ¶ 9.7. Anthem will provide these government officials with all required materials so that the states and federal government may make an independent evaluation of the settlement and bring any concerns to the Court's attention prior to final approval.

D. <u>Appointment of a Settlement Administrator</u>

In connection with the Court's preliminary approval of the Settlement, the parties are also asking the Court to appoint Kurtzman Carson Consultants, LLC ("KCC") to serve as Settlement

Administrator. KCC has over a decade of experience serving as a Settlement Administrator in many large and complex class action lawsuits, including in other data breach lawsuits in which it handled similar duties with respect to assisting class members avail themselves of credit monitoring services, and resolving claims for out of pocket expenses. Cervantez Decl. Ex. C. The cost of notice and claims administration – anticipated to be approximately $23 million, the vast bulk of which is direct mail postage to 50 million Settlement Class Members and pre-paid postage return cards to request credit monitoring services – will be drawn from the Settlement Fund, and will serve not only to inform Settlement Class Members of their due process rights to object or opt out, but to inform them of the important credit monitoring services and other valuable compensation of which they can and should avail themselves. *See, e.g.*, SA Ex. 5a.

E. The Schedule for Final Approval

The next steps in the settlement approval process are to schedule a final approval hearing, notify the class of the Settlement and hearing, allow class members an opportunity to file any objections or comments regarding the Settlement, and allow the parties to conduct appropriate objector discovery, if necessary. *See, e.g., In Re: MagSafe Apple Power Adapter Litig.*, 2015 WL 428105, at *2 (N.D. Cal. Jan. 30, 2015) (objector depositions authorized to inquire into objectors' membership in the class and ability to post an appellate bond). Accordingly, Plaintiffs have provided an agreed-upon proposed schedule in their Motion for Preliminary Approval.

IV. CONCLUSION

Plaintiffs respectfully request that the Court enter the accompanying Proposed Order certifying the proposed settlement class; granting preliminary approval of the proposed settlement; directing dissemination of notice to the class pursuant to the proposed notice plan; appointing a Settlement Administrator for the dissemination of notice and establishment of a Settlement Fund; and setting a schedule for final approval and related deadlines.

Respectfully Submitted,

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

Dated: June 23, 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: June 23, 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