NORMAN E. SIEGEL (*pro hac vice*)
siegel@stuevesiegel.com
J. AUSTIN MOORE (*pro hac vice*)
moore@stuevesiegel.com
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Telephone: 816-714-7101
Facsimile: 816-714-7101

DANIEL C. GIRARD (SBN 114826)
dcg@girardgibbs.com
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, CA 94108
Telephone: 415-981-4800
Facsimile: 415-981-4846

Attorneys for Plaintiffs and the Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN FRANCISCO

MATTHEW PAGOAGA and ANTHONY JONES, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

STEPHENS INSTITUTE d/b/a ACADEMY OF ART UNIVERSITY,

Defendant.

STEPHENS INSTITUTE d/b/a ACADEMY OF ART UNIVERSITY,

Cross-Complainant,

v.

NAVISITE, LLC,

Cross-Defendant.

Case No. CGC 16-551952

DECLARATION OF NORMAN E. SIEGEL IN SUPPORT OF PLAINTIFFS' MOTION FOR FINAL APPROVAL OF CLASS ACTION SETTLEMENT

Judge:	Curtis E.A. Karnow
Dept.:	304
Action Filed:	May 11, 2016
Hearing:	July 16, 2018 at 9:00 a.m.

I, Norman E. Siegel, hereby declare under penalty of perjury pursuant to California Code of Civil Procedure § 2015.5 as follows:

1. I am an attorney in good standing of the State Bar of Missouri and a partner in the law firm Stueve Siegel Hanson LLP. I represent Plaintiffs Matthew Pagoaga and Anthony Jones in this action and submit this declaration in support of Plaintiffs' Motion for Final Approval of the Class Action Settlement. I have knowledge of the facts presented in this Declaration based on my involvement in prosecuting this litigation since its inception.

Procedural History and Settlement Negotiations

2. In April 2016, Academy of Art University ("AAU") announced that it suffered a data breach after one of its employees was targeted by an e-mail "spoofing" scam and sent the 2015 Internal Revenue Service Wage and Tax Statements ("W-2 Forms") of current and former AAU employees to an unknown third party (the "Email Security Incident"). The information contained on the W-2 Forms included, among other sensitive information, employees' full names, addresses and ZIP codes, dates of birth, wage information, and Social Security Numbers. The class consists of 3,373 individuals.[1]

3. On May 11, 2016, my firm filed this putative class action on behalf of Plaintiff Matthew Pagoaga, a former employee of AAU, asserting causes of action for negligence and violations of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et. seq*., and seeking declaratory relief. Plaintiff Pagoaga sought to represent a class of former and current employees of AAU affected by the Email Security Incident.

4. Shortly after the case was filed, counsel for Plaintiffs and AAU's former counsel Zuzana Ikels of Polsinelli LLP began engaging in preliminary settlement discussions. In my experience, early settlements can be especially beneficial in the data breach context because class members can benefit immediately from protections like injunctive relief and credit monitoring services that can help detect and prevent identity theft and fraud before misuse occurs.

[1] Earlier settlement filings reflected the class size as 3,374 individuals. It has since been confirmed that the class list included one duplicate entry, making the settlement class 3,373 individuals.

5. The parties entered into a stand-still agreement that included multiple stipulations to extend AAU's deadline to respond to the Complaint by 120 days so that the parties could explore the possibility of settlement.

6. During this period, the parties regularly communicated on issues relating to settlement and agreed to exchange information necessary to facilitate those discussions, including class member information, detailed information concerning how the breach occurred, the scope and number of individuals affected, the types of injuries suffered by affected individuals, the actions AAU took in response to the breach, and information relating to AAU's vendors retained to handle, create, and secure emails and data, among other relevant information.

7. On July 26, 2016, Plaintiffs' counsel met with AAU's counsel and a representative from AAU in San Francisco, California to discuss the structure of a possible settlement. Following that conference, and at AAU's request, we prepared a formal settlement demand and delivered it to AAU's counsel on August 15, 2016. The demand consisted of three primary components of relief, all of which were included in the parties' ultimate settlement: (1) three-bureau credit monitoring for all class members; (2) reimbursement to class members with out-of-pocket-losses relating to the breach; and (3) business practice changes including the implementation of technical security barriers and an employee cybersecurity training program.

8. In or about October 2016, AAU replaced Ms. Ikels with the firm currently representing AAU. Once AAU's new counsel was up to speed on the litigation, Plaintiffs engaged in continued settlement discussions with AAU's new counsel, and the parties filed a joint stipulation to suspend all deadlines by an additional 21 days to determine if settlement could be reached.

9. On October 28, 2016, Class Counsel provided to AAU's counsel a proposed term sheet setting forth the essential terms of settlement that largely tracked the settlement ultimately agreed to by the parties. Despite the fact that the parties had been negotiating around the same terms for over 3 months, AAU opted not to move forward with settlement, in part because AAU elected to seek contribution from its cybersecurity provider, NaviSite, LLC.

10. After AAU's decision to forego participating in settlement discussions in Fall 2016, Plaintiffs moved forward with discovery efforts. On December 1, 2016, Plaintiffs propounded 32 document requests on AAU.

11. On January 3, 2017, AAU filed a Cross-Complaint against NaviSite for breach of contract, negligence, contractual indemnification, equitable indemnification, partial equitable indemnification, and declaratory relief. NaviSite subsequently filed a demurrer to the Cross Complaint.

12. On January 25, 2017, Plaintiffs noticed AAU for a person most knowledgeable deposition and served interrogatories on AAU.

13. An additional civil action addressing the breach was filed in this Court on October 18, 2016. *See Anthony Jones v. Academy of Art University Foundation*, Case No. CGC-16-554902. Plaintiffs' counsel reached an agreement with counsel for Mr. Jones to dismiss the Jones matter without prejudice, and Plaintiff Jones joined this action via a First Amended Complaint, which Plaintiffs filed on January 20, 2017.

14. AAU served its responses and objections to the Plaintiffs' requests for production of documents on January 26, 2017. To facilitate the exchange of documents, the parties negotiated a protective order that this Court entered on February 22, 2017.

15. In March 2017, AAU responded to Plaintiffs' interrogatory requests and produced approximately 2,300 pages of documents relating to the breach. In conjunction with the preliminary discovery exchanged by parties, AAU's document production and discovery responses permitted Plaintiffs' counsel to more fully weigh the merits of the case and engage in informed settlement negotiations on behalf of the Class.

16. Specifically, the primary factual bases for Plaintiffs' claims were confirmed in the discovery process, including that there were breakdowns in AAU's technical security barriers that permitted an AAU employee to receive the "spoofed" e-mail (this is also detailed in AAU's Cross Complaint against NaviSite), as well as a lack of employee training on how to recognize fraudulent e-mails and best practices regarding intra-company data transfers. Discovery also confirmed that several class members experienced identity theft and fraud in the immediate

aftermath of the Email Security Incident, and while AAU attempted to address these issues on an *ad hoc* basis, there was no uniform policy communicated to affected individuals regarding how to request reimbursement for losses relating to the Email Security Incident.

17. The documentation AAU produced in this litigation demonstrated the types of harms suffered by class members. I included as Exhibit 2 to my Declaration in Support of Plaintiffs' Renewed Motion for Preliminary Approval filed on November 11, 2017 documentation produced by AAU in this litigation, including complaints from class members, which set forth examples of harm experienced by class members in the aftermath of this breach. It included:

a. Several employees had a tax return fraudulently filed using their name and sought advice about how to handle the situation (Docs. 000742, 753, 758);

b. An employee asked how to stop automatic deposit of her paycheck because she closed her bank account as a safety precaution (Doc. 000675);

c. An employee emailed AAU stating: "Given the recent identity breach at AAU, I would like to place a security freeze with all three credit bureaus. This costs a total of $30. Is the Academy willing to reimburse me for this cost?" (Doc. 000740);

d. An employee sought reimbursement for costs associated with having an accountant resubmit her tax return after having a fraudulent tax return filed in her name (Doc. 000742);

e. An employee complained of suspicious calls in the aftermath of the breach and sought guidance on whether she should file an identity theft affidavit with the IRS (Docs. 000743-744);

f. An employee sought reimbursement for purchasing one year of LifeLock Ultimate Plus credit monitoring in the amount of $296 (Doc. 000749);

g. An employee sought reimbursement for accountant fees in the amount of $447.95 and $117.00 associated with preparing an IRS identity theft affidavit and filing a paper copy of tax return after fraudulent return filed (Docs. 000753-55); and

h. An employee had a fraudulent mortgage filed in his name which resulted in him closing his bank accounts and incurring a $65 charge for uncleared checks (Docs. 000758-60).

18. On April 13, 2017, this Court entered an order sustaining in part and overruling in part NaviSite's demurrers to the Cross Complaint with leave to amend. Following that ruling, and in advance of Plaintiffs' motion for class certification, all parties agreed to participate in a joint mediation session before a mediator experienced in complex litigation. Plaintiffs agreed to continue the PMK depositions and class certification deadlines until after participating in a formal mediation.

19. On April 25, 2017, counsel for Plaintiffs, AAU and NaviSite participated in a formal mediation session before a mediator experienced in complex litigation, Cathy Yanni of JAMS ADR in San Francisco, California. While the parties were not able to reach an agreement at that session, the parties continued to engage in post-mediation settlement discussions through Ms. Yanni and directly between counsel.

20. On June 9, 2017, the parties filed a joint stipulation and proposed order to continue class certification deadlines informing the Court that the parties were close to settlement.

21. Thereafter, AAU and NaviSite reached an agreement to settle the Cross-Complaint. Following that agreement, Plaintiffs and AAU agreed on the essential terms of a settlement and accepted the term sheet proposed by Plaintiffs. On July 7, 2017, after more than a year of negotiations, Plaintiffs and AAU filed a joint notice of settlement.

Preliminary Approval Process

22. On September 20, 2017, the Court held a hearing on Plaintiffs' unopposed motion for preliminary approval of the settlement. The Court denied the motion without prejudice and requested clarification of several issues related to the settlement.

23. Plaintiffs thereafter renegotiated several aspects of the settlement with AAU, revised the class notice and claim forms in accordance with the direction offered by the Court, and prepared a renewed motion for preliminary approval. As part of that filing, Plaintiffs provided the Court with supplemental information regarding the types of harm likely to be experienced by class

members with accompanying exhibits, a summary of documentation produced by AAU in the litigation (summarized above), an explanation as to the benefits of the credit monitoring and fraud resolution services offered under the settlement, and more information regarding the claims process and contractual business commitments undertaken by AAU.

24. The renewed motion came for hearing on January 16, 2018. On that same day, the Court issued an order continuing the motion so that the parties could address several additional issues raised by the Court. *Id*. In response, the parties agreed to add more clarity to several aspects of the Settlement including further defining the "fairly traceable" standard for assessing claims and adding more specificity to AAU's cybersecurity training requirements. On February 13, 2018, the Court granted the renewed motion for preliminary approval.

Overview of the Settlement

25. The Settlement includes multi-faceted relief that is designed to address past, present and future harm, including the following: (1) AAU will reimburse settlement class members for documented out-of-pocket losses fairly traceable to the E-mail Security Incident, up to $1,000 per individual, or $2,500 per individual with receipt for the purchase of professional services, including accountant and attorneys' fees; (2) class members are also eligible to enroll in two years of Experian's three-bureau "3B Credit Plus" credit monitoring services at no cost, regardless of whether the class member submits a claim for reimbursement of out-of-pocket losses; (3) all class members will be eligible to take advantage of identity restoration services offered through Experian, including professional fraud resolution assistance to help with identity recovery and restoration in case the class member experiences identity theft or fraud in the future, regardless of whether they make a claim under the Settlement; and (4) AAU will make changes to its business practices, including implementing technical security barriers to limit the flow of fraudulent e-mails and maintaining an employee cybersecurity training program.

Reimbursement for Out-of-Pocket Losses

26. The Settlement is structured to permit class members to submit documentation for reimbursement of out-of-pocket losses and unreimbursed charges fairly traceable to the breach up to $1,000 per individual for out-of-pocket losses not including the purchase of professional

services and in addition, $2,500 per individual for out-of-pocket losses consisting only of the purchase of professional services, including accountant and attorneys' fees. The maximum amount payable for reimbursement by AAU is $250,000.

27. The parties agreed that out-of-pocket losses may include, without limitation, unreimbursed fraud losses or charges, professional fees incurred in connection with identity theft or falsified tax returns, credit freezes, credit monitoring that was purchased on or after April 5, 2016 through the date on which the credit monitoring services become available through the Settlement, and miscellaneous expenses such as notary, fax, postage, copying, mileage, and long-distance telephone charges. Agreement, ¶ 16.

28. In assessing what qualifies as "fairly traceable," the parties agreed to instruct the Settlement Administrator to consider the (i) timing of the loss including whether it incurred after the breach, and (ii) the nature of the loss including whether mitigation costs were reasonably incurred and/or whether the information used to commit identity theft or fraud consisted of the same information that was compromised in the breach. *See id*., ¶ 34. The parties further agreed that costs expended for credit monitoring services, credit freezes, and professional services incurred to address identity theft or fraud after the breach shall be presumed "reasonably incurred." *See id*., ¶ 34. If the claim is rejected for any reason, the parties committed to a consumer-friendly appeals process whereby claimants will have the opportunity to cure any deficiencies in their submission or request an automatic appeal if the Settlement Administrator determines a claim for out-of-pocket losses is deficient in whole or part.

29. The Settlement is also structured to compensate losses from identity theft or fraud that may occur in the future. Class members are permitted to submit claims for reimbursement of out-of-pocket losses for up to 640 days after the claims deadline (known as the "Tail Deadline"), so long as the class member (a) submitted a claim electing to receive the credit monitoring services offered as part of the Settlement on or before the initial claims deadline; and (b) provides an attestation that he or she has not obtained reimbursement for the claimed expense through other means. To our knowledge, this is the first data breach settlement to include an extended, multi-year claims period.

Three-Bureau Credit Monitoring and Identity Resolution

30. All class members are also entitled to receive two years of free, three-bureau credit monitoring services, regardless of whether they submit a claim for out-of-pocket losses. Credit monitoring is a service that monitors an individual's credit reports and alerts the individual when any change is made that could signal fraudulent activity. Credit changes can include new credit card or loan applications, new credit inquiries, existing account changes, and new public records or address changes, among others. Credit monitoring gives the individual the opportunity to confirm the accuracy of a credit change in real time and, if necessary, address the issue before fraud occurs or expands.

31. The features included with Experian's "3B Credit Plus" credit monitoring services include the following:

a. Daily credit monitoring of the class member's credit file at all three (3) major credit reporting agencies (Experian, Equifax & TransUnion);

b. An Experian credit report upon enrollment;

c. A subsequent, updated Experian credit report available (online) at the class member's election as often as daily;

d. Identity theft insurance offered through AIG, which covers certain identity theft related expenses incurred by the class member up to a limit of $1 million;

e. Internet surveillance, which includes monitoring of the "dark web" for the class member's personal information;

f. Identity validation monitoring and alerts to notify the class member in the event his or her identity has been verified across the Experian identity network; and

g. Identity restoration services that provide professional fraud resolution assistance to the class member if he or she experiences identity theft or fraud, helping with identity recovery and restoration.

32. This relief is important for several reasons. First, credit monitoring can help detect fraud before it occurs or expands—an important tool in the aftermath of a breach. Second, it provides class members with access to Experian's fraud resolution agents, who can provide guidance if class members experience fraud or if other issues arise. Experian explains how fraud resolution agents can assist class members who experience suspicious activity or fraud:

We will follow these six steps to protect you from the damages caused by identity theft:

1. **Notify banks, creditors and service providers**: We'll be on the phone with you to assist with notifying your creditors, medical benefits company, your bank or other financial institutions, and your utilities. And if correspondence by mail is required, we'll draft letters for you to sign.
2. **Place fraud alerts on your credit report**: We'll help you place an immediate, 90-day alert on your credit report at all three major credit bureaus, to warn lenders and other potential credit grantors that you may be a victim of identity theft. Plus, we'll help you renew the fraud alert if necessary, or add a 7-year alert if your identity proves to have been stolen.
3. **Report the fraud to government agencies**: We walk you through the steps of contacting your local law enforcement agency to file a report regarding the fraudulent activity. This report becomes your official "Identity Theft Report" a document that creditors and credit bureaus may ask for. If you wish to file a report with the Federal Trade Commission, we'll help you with that too.
4. **Check your credit reports**: In the event of an identity theft, we'll review your Experian® bureau, TransUnion and Equifax files with you so we can help you identify possible fraudulent activity you may be unaware of. We'll immediately get started helping you resolve any issues we find.
5. **Cancel or request new credit, debit or insurance cards**: Depending on the situation, you may need to cancel or change some or all of your accounts as a result of the identity theft. We'll help you determine which accounts to close. We'll guide you through contacting your card issuers, medical benefits companies and/or financial institutions to close your current accounts, report stolen checks, stop payments on outstanding checks you've written (if necessary) and transfer any recurring charges from your old accounts to new ones.
6. **Secure and reclaim your identity**: We'll help you gather the necessary information you'll need to make telephone calls or to send letters to your creditors, your bank, the credit bureaus, and any others who may be involved in the process of securing and reclaiming your identity."[2]

33. Experian confirms that their fraud resolution agents are U.S.-based employees[3] and that they "receive a minimum of 10 weeks of intensive training in fraud resolution. Each agent is certified under the federal Fair Credit Reporting Act (FCRA). Plus, they receive continual support and training from the nationally recognized non-profit Identity Theft Resource Center (ITRC)." [4] Experian represents that: "We don't put our agents on the phone with your customers unless they've proven themselves in resolving identity theft."[5]

34. As a separate class benefit, all class members – including those who do not enroll

[2] http://www.experian.com/data-breach/data-breach-faq.html#faq12.
[3] http://www.experian.com/data-breach/data-breach-faq.html#faq11.
[4] http://www.experian.com/data-breach/data-compromise.html.
[5] *Id*.

in credit monitoring services or otherwise submit a claim – will be entitled to utilize the identity restoration services through Experian by referencing a unique engagement code. This coverage permits all class members, even those who do not submit a claim, to have access to fraud resolution specialists who can assist with important tasks such as placing fraud alerts with the credit bureaus, disputing inaccurate information on credit reports, scheduling calls with creditors and other service providers, and working with law enforcement and government agencies to dispute fraudulent information. The identity restoration services will be available for a period of two years from the effective date of settlement.

35. Finally, the credit monitoring services offered as part of this Settlement provide significant value to the class. Experian offers a comparable consumer service that retails for $19.99 per month.[6] Other comparable services offered by leading credit monitoring providers IdentityGuard and LifeLock retail for $24.99[7] and $29.99[8] per month, respectively.

36. As part of this Settlement, the parties were able to negotiate a group discount whereby AAU is obligated to pay $61.12 per class member who elects credit monitoring as a settlement benefit on their claim form (regardless of whether they ultimately enroll) for two years of coverage, and an additional flat fee of $10,324.44 to provide everyone in the class access to Experian's fraud resolution agents (regardless of whether the services are used).

37. While the fact that the parties were able to negotiate a discounted rate for these services made settlement feasible, the actual market value of this settlement benefit can fairly be estimated at $480 per class member ($19.99 per months for 24 months), which is the lower-end price for these services on the open market. This equates to a settlement benefit of over $1.6 million to the class as a whole.

Contractual Business Practice Commitments

38. As part of the Settlement, AAU has agreed to implement certain business practice changes intended to better secure the personal information of class members. The Settlement

[6] https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html.
[7] https://www.identityguard.com/compare-plans/platinum/.
[8] https://www.lifelock.com/products/lifelock-ultimate-plus/.

Agreement provides that within 30 days of the effective date, AAU must provide to Plaintiffs' counsel documentation establishing that AAU has implemented (1) technical security barriers specifically designed to reduce the flow of unwanted outside e-mails (common examples include Sender Policy Framework, DomainKey Identified Mail, and/or Domain-based Message Authentication); and (2) an employee cybersecurity training program that trains and educates employees responsible for handling payroll and compensation data on maintaining the confidentiality of such information, and helping them recognize scams aimed at gaining unauthorized access to such information, including "phishing" and "spoofing" scams. The cybersecurity training shall be delivered on an annual basis, and will also be included in the onboarding process for new employees responsible for handling payroll and compensation data. Agreement, ¶ 43.

39. If at any time during three years from the effective date Plaintiffs' counsel have questions regarding the documentation submitted by AAU or believe that AAU is not complying with its contractual business practice commitments, the parties are required to meet and confer to discuss the issue. Agreement, ¶ 44. If after meeting and conferring Plaintiffs' counsel believes that AAU is not adhering to its contractual obligations, Plaintiffs may then file a motion with the Court to seek further discovery or enforce the Settlement Agreement. The Court will retain jurisdiction for this purpose for three years from the effective date. *Id*.

Valuing the Settlement and Risks of Continued Litigation

40. As set forth in my prior declarations, in most instances, victims of a data breach do not have any immediate harm such as identity theft or fraud, or if they do, they are not financially responsible for it because financial institutions commonly bear that risk. What victims do complain of, however, is a lack of sufficient information and guidance about how to protect themselves in the wake of a breach and how to address issues when they arise. Accordingly, in my experience, the most common complaint from victims of a data breach is a lack of knowledge about how to detect or prevent identity theft and fraud, and how to address it when it occurs.

41. When a victim incurs out-of-pocket expenses relating to a data breach, it is typically associated with seeking advice about how to address the breach (*e.g.*, paying for

professional services), paying incidental costs associated with identity theft or fraud (*e.g.*, overdraft fees or costs for sending documents by certified mail), or taking mitigative measures like paying for credit monitoring or credit freezes. As such, the out-of-pocket expenses associated with a data breach are generally relatively low, and rarely exceed several hundred dollars. When victims spend more than this amount, it is typically associated with paying for professional services such as accountant or attorneys' fees. Future out of pocket damages are often mitigated or eliminated with the protections offered through monitoring services like the type provided in this Settlement.

42. The limited research available supports this conclusion. Included as Exhibit 1 to my Declaration in Support of Plaintiffs' Renewed Motion for Preliminary Approval filed on November 11, 2017, was a study conducted by the Ponemon Institute,[9] a company that conducts independent research on privacy, data protection and information security policy. The study found that in the aftermath of a data breach, 81% of data breach victims do not have any out-of-pocket losses, and for the 19% that do, those losses average to $38 per individual.

43. Using the Ponemon research as a baseline, I previously estimated that if approximately 19% of class members suffer losses after a data breach, with average losses of $38 each, the out-of-pocket-losses in this case would total approximately $24,358 if every class member participated in the Settlement.

44. Given this data, and my firm's experience in similar data breach litigation, Plaintiff was agreeable to imposing individual caps of $1,000 and $2,500, respectively, for reimbursement of out-of-pocket losses because the vast majority of losses incurred in the aftermath of a breach are well under $1,000, as demonstrated by the discovery produced in this case. When victims exceed the $1,000 threshold, it is typically because they paid for professional services such as accountant or attorneys' fees. Thus, the parties agreed to increase the cap to $2,500 when professional fees were incurred.

[9] Larry Ponemon, founder of the Ponemon Institute, served as an expert witness for class action plaintiffs in two of the largest retail data breach cases in U.S. history, *In re: Target Corp. Customer Data Sec. Breach Litig.*, Case No. 0:14-md-02522 (D. Minn.) and *In re: Home Depot, Inc. Customer Data Sec. Breach Litig.*, Case No. 1:14-md-02583 (N.D. Ga.).

45. With respect to the $250,000 overall cap, AAU insisted that its insurer needed to account for its maximum possible exposure. After extensive negotiations, Plaintiffs' counsel agreed to a cap of $250,000 because, based on the research available and our experience in similar litigation, we did not believe the amount of approved claims for out-of-pocket losses will approach this limit.

46. After analyzing the claims data, Plaintiffs predictions were essentially correct. Only one class member submitted a claim with damages exceeding the $2,500 individual cap, and she opted to make a claim rather under the Settlement rather than opt-out and pursue an individual action. The total of all out-of-pocket losses approved by the Settlement Administrator was $10,307.84, meaning there is no danger of hitting the $250,000 cap, and all verified claims submitted during the tail period will be eligible for full reimbursement.

47. To determine whether this Settlement is in the "ballpark" of reasonableness (*Kullar v. Foot Locker Retail, Inc*. 168 Cal.App.4th 116, 133 (Cal. Ct. App. 2008)), the Court may compare the relief offered as part of this Settlement to Plaintiffs' maximum possible recovery had everything gone their way through trial.

48. At trial, Plaintiffs would ideally seek at trial compensatory damages for the costs of purchasing two years' worth of high-level credit monitoring services for each member of the class (estimated above at $480 per class member), plus any additional out-of-pocket losses experienced by class members (estimated above at $24,358 for the entire class). This would make Plaintiffs' maximum possible recovery at trial approximately $1,643,878.

49. But the legal support for recovery of these types of damages is uncertain and would be hotly-contested. Negligence damages require a showing of "concrete loss" under California law. *See Bardis v. Oates*, 119 Cal. App. 4th 1, 17, 14 Cal. Rptr. 3d 89, 101 (Cal. Ct. App. 2004) ("Compensatory damages are intended to redress the concrete loss that the plaintiff has suffered by reason of the defendant's wrongful conduct."). This means that the plaintiff is entitled to be in the same financial position that she would have been had the accident not occurred. *See Tremeroli v. Austin Trailer Equip. Co.*, 227 P.2d 923, 934 (Cal. Ct. App. 1951).

50. AAU would assuredly argue that class members who did not actually spend money on mitigation efforts (or otherwise suffer out-of-pocket losses) would not be permitted to recovery anything because they have no actual damages. Plaintiffs are unaware of any cases where such mitigative damages have been sought at trial.

51. While the law on this issue is undeveloped, recovery at trial it is certainly fraught with risk given that the class may not recover anything despite the high costs and delay of further discovery, motion practice, trial, and appeal. This of course assumes Plaintiffs would make it to trial given that class certification has been denied in other data breach cases. *See, e.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 293 F.R.D. 21 (D. Me. 2013) (denying class certification because individualized proof would be required to ascertain each class member's damages).

52. As part of this Settlement, each class member will receive two years of free, high-level credit monitoring that has a retail value of $480 per class member. These services will assist class members in addressing the real world effects from the breach, including real-time monitoring of their credit and human assistance. In addition, class members with out-of-pocket losses can receive full reimbursement for any money they expended fairly traceable to the breach. And, while not assigned a monetary value, AAU is contractually required to implement business practice changes designed to make class members' information more secure. Accordingly, every one of the actual examples of harm traceable to this breach, including injuries sustained by the named plaintiffs as well as other class members who contacted AAU, are addressed in this Settlement.

53. The Court does not need to determine the exact dollar "value" of the Settlement in order to conclude that the "recovery represents a reasonable compromise, given the magnitude and apparent merit of the claims being released, discounted by the risks and expenses of attempting to establish and collect on those claims by pursuing the litigation." *Kullar*, 168 Cal. App. 4th at 129. Comparing the Settlement benefits with total maximum value of this case, while at the same time

weighing the risks involved in pursuing class certification and an undeveloped damages theory, this Settlement is well within the "ballpark of reasonableness."[10]

The Settlement is Well-Supported by Class Members and Counsel

54. Since the revelation of the Target data breach in late 2013, much of my practice, along with that of my colleague Austin Moore, has been dedicated to representing victims of data breaches. I co-founded the American Association for Justice's Consumer Privacy and Data Breach Litigation Group and previously served as the group's co-chair. I am a nationally published author on emerging issues impacting data breach cases, and I regularly speak on data breach litigation issues.

55. My experience in data breach and consumer privacy cases includes appointment as a member of the executive committee in *In Re: Target Corporation Customer Data Security Breach Litigation*, No. 14-md-2522 (D. Minn.) (involving breach affecting tens of millions of customers), before the Hon. Paul A. Magnuson (D. Minn.) and as co-lead counsel for consumer plaintiffs in *In Re: The Home Depot, Inc., Customer Data Security Breach Litigation*, No. 14-md-02583 (N.D. Ga.) (involving breach affecting more than 60 million customers).

56. In the *Home Depot* litigation, I served as the principal negotiator on behalf of the consumer class which resulted in a settlement that the presiding judge, the Honorable Thomas W. Thrash, referred to as an "exceptional result" and "the most comprehensive settlement achieved in large-scale data breach litigation." *In re: The Home Depot, Inc., Customer Data Security Breach*

[10] Similarly, AAU has agreed to pay the reasonable attorneys' fees, costs and expenses of Plaintiffs' counsel in prosecuting this action, which, as set forth more fully in Plaintiffs' Motion for Attorneys' Fees and Costs, should be determined using the lodestar-multiplier method. *See Carr v. Tadin, Inc*., 51 F. Supp. 3d 970, 978 (S.D. Cal. 2014) ("because there is no common fund, the lodestar analysis applies to Class Counsel's request."). "Under the lodestar method, a fee award need *not* bear any specific proportionality to the dollar amount of the recovery. *Britto v. Zep Inc*., No. A141870, 2015 WL 5657147, at *16 (Cal. Ct. App. Sept. 25, 2015) (emphasis in original); *see also Taylor v. Nabors Drilling USA, LP*, 222 Cal. App. 4th 1228, 1251 (Cal. Ct. App. 2014) (no authority "requiring that fee awards be proportional to the amount of damages recovered"); *Harman v. City & Cty. of San Francisco*, 158 Cal. App. 4th 407, 421 (Cal. Ct. App. 2007) ("There is no mathematical rule requiring proportionality between compensatory damages and attorney's fees award"). For this reason too, the Court need not determine the exact dollar "value" of the Settlement in order assess the reasonableness of attorneys' fees.

Litigation, Case 1:14-md-02583-TWT, Doc. 261 at *3 (N.D. Ga.), attached as Exhibit F to my declaration in support of Plaintiffs' motion for attorneys' fees and costs.

57. In February 2018, I was appointed as co-lead counsel in the largest data breach case to date, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 1:17-md-2800-TWT (N.D. Ga.), which stemmed from a massive breach that compromised highly-sensitive information of more than 145 million consumers. In addition to the above cases, Mr. Moore and I are counsel in *In Re: Anthem, Inc. Data Breach Litigation*, No. 15-md-02617 (N.D. Ca.) (involving breach of up to 80 million members' health records); *In Re: U.S. Office of Personnel Management Data Security Breach Litigation*, No. 1:15-mc-01394-ABJ (D.D.C.) (involving breach of private records of 21.5 million current, former and prospective government employees and contractors); and *Liang, et al. v. Nat'l Board of Examiners in Optometry, Inc*., No. 1:17-CV-1964 (D. Md.) (testing board breach affecting thousands of optometrists across the country).

58. Mr. Moore has worked closely with me in each of these cases and has developed considerable expertise in this practice area. He has particular insight on the types of relief viewed as beneficial to victims of a data breach having led nationwide plaintiff vetting efforts in several data breach MDLs and having interviewed literally thousands of data breach victims over the last 4 years. The Settlement in this case was specifically structured to include the types of relief that data breach victims are most likely to find beneficial.

59. As a result of our collective experience in this practice area, we were able to propose and eventually negotiate a settlement that was structured to include the types of relief that data breach victims are most likely to benefit from and that is specifically tailored to the facts of this case. It is our view that given the multi-faceted relief made available, this Settlement compares very favorable to other data breach settlements made in the last five years.

60. This Settlement has also received an overwhelmingly positive reaction from the class. After a 90-day initial claims period, no class members have objected to the Settlement, and only three out of 3,373 (or .08%) class members have requested exclusion.

61. Additionally, more than 7.2% of *verified* class members made claims under the Settlement during the initial claims period. Although case dependent, in my experience consumer

class action settlements typically have a claims rate between 3-5%, and claims rates in data breach settlements are even lower given the relatively low dollar value of the claims. The strong class participation further supports the fairness and adequacy of the Settlement.

I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed this 21st day of June, 2018, in Kansas City, Missouri.

Norman E. Siegel