

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MARIE ABDELMESSIH, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

FIVE BELOW INC.

Defendant.

Case No.: 2:19-cv-1487

**PLAINTIFF'S SUPPLEMENTAL
MEMORANDUM IN SUPPORT OF
MOTION FOR PRELIMINARY
APPROVAL**

As discussed at the March 26, 2020, hearing, and as instructed by the Court's March 31, 2020, Order (Doc. 30), Plaintiff, Marie Abdelmessih ("Plaintiff"), provides this supplemental brief in support of her Motion for Preliminary Approval, (Doc. 26).¹

At the hearing, the Court raised concerns regarding (1) the harm Plaintiff alleged to have incurred in the complaint, (2) the damages Plaintiff would seek at trial, and, (3) based thereon, whether the compensation to the class established by the Settlement Agreement is sufficient. The Court also referenced some potential concerns regarding the length and complexity of the Claim Form. As explained below, the compensation proposed by the Settlement fits closely to the allegations of harm set forth in the Complaint, and based on counsel's significant experience with other data breach cases, and concomitant understanding of expected claim's rates and claimed amounts, the proposed Settlement should provide adequate funds to compensate the valid claims made against it. The Parties have also streamlined the Claim Form to make filing a claim by Class Members as straightforward and simple as possible.

¹ Unless otherwise defined, capitalized terms have the same meaning attributed to them in the Settlement Agreement, previously filed at Doc. 26-1, and cited to as "S.A."

I. DISCUSSION

A. Harms Alleged in the Complaint are Compensated for by the Settlement

In the Complaint, Plaintiff alleges various types of harm that the class suffered, including fraudulent credit and debit card charges (Doc. 1 at ¶ 51); and a real, concrete, and actual risk of future identity theft and identity fraud requiring Plaintiff and Class Members to take the time to mitigate the actual and potential impact of the Data Breach, (*id.* ¶¶ 56–57). The gravamen of Plaintiff’s class-wide harm allegations is encapsulated at paragraphs 63 and 64:

63. As a result of the Defendant’[s] failures to prevent the Data Breach, Plaintiff and Class members have suffered and will continue to suffer damages. They have suffered, or are at increased risk of suffering:

- a. The compromise, publication, theft and/or unauthorized use of their PCD/PII;
- b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- c. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- d. The continued risk to their PCD/PII, which remains in the possession of the Defendant and is subject to further breaches so long as the Defendant fails to undertake appropriate measures to protect the PCD/PII in their possession; and
- e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of Plaintiff’s and Class members’ lives.

64. Additionally, Defendant continues to hold the PCD/PII of its customers. Particularly, because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PCD/PII is secure, remains secure, and is not subject to further theft.

(Doc. 1 at ¶¶ 63–64). As to Plaintiff specifically, she experienced attempted transfers of funds from her accounts, requiring her to spend hours of her time in an effort to stop the fraud from

continuing and to prevent it from reoccurring, including contacting her bank's fraud department, filing a police report, speaking with the grocery store manager where fraudulent transactions were attempted, contacting the three major credit bureaus to freeze her credit, and visiting her bank to open new accounts, reset passwords, and obtain a new Visa card. (Doc. 1 at ¶ 12).

The Settlement (1) addresses precisely the types of harms alleged in the Complaint, and is based on Plaintiff counsel's experience from speaking with consumers following data breaches of this type, and (2) rectifies the ongoing concern regarding how Defendant is protecting the payment card data ("PCD") and personally identifiable information ("PII") of its customers.

First, the Settlement provides compensation for the kinds of out-of-pocket costs and lost time the complaint alleged were at issue:

- Settlement Class Members are eligible for reimbursement of expenses, up to \$250 per Settlement Class Member, that were incurred as a result of the Security Incident. Reimbursable expenses include: (i) unreimbursed bank fees; (ii) unreimbursed card reissuance fees; (iii) unreimbursed overdraft fees; (iv) unreimbursed charges related to unavailability of funds; (v) unreimbursed late fees; (vi) unreimbursed over-limit fees; (vii) long distance telephone charges; (viii) cell minutes (if charged by minute), Internet usage charges (if charged by the minute or by the amount of data usage and incurred solely as a result of the Security Incident), and text messages (if charged by the message and incurred solely as a result of the Security Incident); (ix) unreimbursed charges, including fraudulent charges, from banks or credit card companies; (x) postage; (xi) interest on payday loans due to card cancellation or due to over-limit situation; and (xii) costs of credit report(s) purchased by Settlement Class Members. S.A. ¶¶ 2.1, 2.1(a).

- Lost time—a prominent issue for Class Members in responding to any data breach as illustrated by the Complaint’s allegations and the Plaintiff’s experience here—is also compensable under the Settlement, with Class Members that have documented fraudulent charges eligible for up to five (5) hours, calculated at the rate of \$20 per hour; and Class Members without documented fraudulent charges eligible for up to three (3) hours of time, calculated at the rate of \$20 per hour, for time spent dealing with replacement card issues or otherwise dealing with the Security Incident. S.A. ¶ 2.1(b)(i), (ii).
- Moreover, Class Members with documented fraudulent charges are also eligible for a \$22 payment for each credit or debit card on which documented fraudulent charges were incurred, even where those charges were ultimately reversed. S.A. ¶ 2.1(c).

Thus, the kinds of out-of-pocket costs and lost time that the Complaint alleged as at issue here are compensated for under the Settlement.

Next, under the Settlement, Defendant agrees to provide Plaintiff confirmation that it has adopted certain data security measures, including, hiring a dedicated IT security employee, and that, on annual basis, it has implemented penetration testing, employee training related to data security, and an annual audit conducted by a Qualified Security Assessor for compliance with the Payment Card Industry Data Security Standard. Defendant agrees to provide Plaintiff information about these practices for a period of three years following the execution of the Settlement Agreement. S.A. ¶ 2.4.

Accordingly, there is an exceedingly close fit between the harms and concerns alleged in the Complaint and the remedies provided by the Settlement.

B. Other Damages Models

At the hearing the Court also inquired as to potential maximum recoveries at trial. That analysis necessarily entails an examination of class certification issues—given that subject matter jurisdiction here is based on the Class Action Fairness Act, and thus this case would only proceed to trial before this Court if a class were certified. In data breach cases especially, the most consistently contentious issues for certification of a damages class—under Rule 23(b)(3), as opposed to an injunctive or declaratory relief class under Rule 23(b)(2)—are commonality under Rule 23(a)(2), and predominance and manageability under Rule 23(b)(3).

Generally, defendants in data breach cases raise the issue that class members’ out-of-pocket costs related to a data breach are necessarily too individualized to permit certification. Whether any particular class member suffered identity theft; if so, establishing a causal nexus between the identity theft of any particular individual and the breach at issue; and then determining the amount of damages arising from the identity theft to each class member, are all links in the evidentiary chain often attacked by defendants at class certification in data breach cases. *See, e.g., Adkins v. Facebook, Inc.*, C 18-05982-WHA, 2019 WL 7212315, at *2 (N.D. Cal. Nov. 26, 2019) (“In opposing the class certification motion, Facebook concentrates most of its fire on the Rule 23(b)(3) damages class. Primarily, Facebook opposes on the ground that individual issues would predominate.”).

Accordingly, plaintiffs in data breach cases also usually provide damages models based on some other discernable measure that is uniform across the class. This can take many forms, but one typical measure is Dark Web pricing for the information at issue. As discussed at the hearing, Dark Web pricing for PCD can vary greatly, depending on a number of factors, including other information associated along with the PCD and the source of the breach from which the PCD was

derived. Generally available sources put Dark Web pricing of payment cards with CVV numbers at about \$5 per card,² which is also what the Complaint references. *See* (Doc. 1 at ¶ 19) (citing Experian data in footnote 2). With a Settlement Class here of approximately 56,000 individuals, that equates to \$280,000.00.

C. The Monetary Consideration in the Settlement Agreement is Fair and Reasonable

Chiefly, at the hearing, the Court seemed most concerned about whether Plaintiff's damages were typical of other Class Members and would the amount made available for claims be sufficient. Here, the Settlement provides for amounts of up to: \$112,000.00 for claims, \$93,750.00 for attorney's fees and costs, and \$1,500.00 for a Service Award; as well separate payment for class notice and administration, which is estimated to cost approximately \$64,000. Combined, this amounts to \$271,250.00. This amount is fair and reasonable when considering (a) the class's likely argument for class-wide recovery at trial, (b) typical damages suffered by Plaintiff and Class Members, and (c) the likely amount of funds that will be claimed as damage by the putative class.

First, as noted above, defendants typically challenge the predominance and manageability elements of Rule 23 when faced with a class seeking the type of identity-fraud-based damages alleged in the Complaint. For example, defense counsel recently defeated a proposed class in a data breach case in which the plaintiff bank sought to recover fraudulent charges it paid on behalf of its customers based on these arguments. *See S. Indep. Bank v. Fred's, Inc.*, No. 2:15-CV-799-WKW, 2019 WL 1179396, at *20 (M.D. Ala. Mar. 13, 2019) (denying certification because determining the "causal link between those losses and the alleged identity theft" would have

² <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (noting dark web price for payment card with CVV number as \$5); <https://www.idtheftcenter.org/how-much-is-your-identity-worth-on-the-black-market/> (“[A] card number with the CVV2 code from the back is worth between \$5-\$8 dollars.”).

required reviewing the individual situations of the bank's "affected customers, numbering in the thousands").

While Plaintiff disputes that these arguments necessarily bar certification of a consumer class,³ nevertheless, Plaintiff must assess and value those risks, and it is certainly possible that the most likely litigated outcome for class certification would be either a Rule 23(b)(3) class seeking a uniform damages model, such as the Dark Web model discussed above; or an injunctive and declaratory relief only class under Rule 23(b)(2), as recently occurred in the Facebook Data Breach case. *See, e.g., Adkins v. Facebook, Inc.*, 2019 WL 7212315, at *9 ("Plaintiff's motion for class certification of a damages class under Rule 23(b)(3) and under Rule 23(c)(4) is DENIED. Plaintiff's motion for class certification of an injunctive class under Rule 23(b)(2) is GRANTED."). Were the latter to happen here, Class Members would not be able to receive any monetary compensation and would be left to pursue individual litigation in order to recover their losses.

And, had a common fund based on Dark Web pricing been obtained at trial, amounts for attorney's fees and costs, a Service Award, and class notice and administration, would have been drawn from the fund. Accordingly, it is fair to compare the total value created by the Settlement (\$271,250.00) against the Dark Web pricing-based hypothetical common fund (\$280,000.00). Thus, the total recovery available in the Settlement nearly matches one of the Class's likely potential outcomes at trial. But even this Dark Web pricing-based theory is not without risk. Defendant disputes the underlying basis for the theory and courts have gone both ways. *Compare In re Marriott International, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL

³ *See, e.g., Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *14 (M.D. Ala. Mar. 17, 2017) (certifying data breach class of approximately 1,000 individuals because causation issues could be addressed on a class basis).

869241, at *7–9 (D. Md. Feb. 21, 2020) (finding theory cognizable), with *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (declining to do so).

The Settlement, however, provides Settlement Class Members the ability to claim amounts significantly in excess of a few dollars, and compensates them for harms that they more acutely feel from a data breach—that is, those described in ¶ 63 of the Complaint. And with a settlement class, the issues associated with Defendant’s individualized objections to each person’s causation and damages are obviated by the agreed-upon claims process. See *In re: Processed Egg Prod. Antitrust Litig.*, No. 08-MD-2002, 2016 WL 3584632, at *8 (E.D. Pa. June 30, 2016) (“[C]ommon questions of fact and law may predominate with regards to a settlement class, while separate individual questions could nevertheless prevent certification of a litigation class.”).

Based on Class Counsel’s review of settlement administration data from more than two dozen data breach settlements in which counsel have been involved, counsel firmly believe the amount made available for claims will be sufficient. The payment card breach matters reviewed included: *In re: Home Depot Customer Data Security Breach Litigation*, No. 14-md-02583 (N.D. GA); *In Re: Arby’s Restaurant Group, Inc. Data Security Litigation*, No. 1:17-cv-1035 (N.D. GA); *Torres et al. v. Wendy’s International LLC*, No. 16-cv-210-PGB-DCI (M.D. Fla.); and *Walters v. Kimpton Hotel & Restaurant*, No. 3:16-cv-05387 (N.D. Cal.). This review included not only payment card breaches—like that at issue here—but also breaches involving far more sensitive data, such as W-2 phishing breaches, where, for example, an employer discloses the W-2 information (including Social Security Numbers) for all its employees to an attacker, often leading to rampant tax return fraud. See, e.g., *Fulton-Green v. Accolade, Inc.*, 2:18-cv-00274-GEKP (E.D. Pa.); *Brady v. Scotty’s Holdings, LLC*, 1:17-cv-01313 (S.D. Ind.); *Linnins v. TIMCO Aviation Services, Inc.*, 16-cv-486 (M.D.N.C.). Plaintiff’s counsel also reviewed data from the W-

2 cases as a comparison for this Settlement because the class sizes in those cases are more reflective of the class size at issue here; typically W-2 cases involve a few hundred to a few thousand class members, whereas the payment card breaches that Plaintiff's counsel typically litigates usually involve in the millions of class members.

All of that data reveals that the total claimed amount in payment card breaches—like this one—averages to less than \$2.00 per class member, and often less than \$1.00 per class member. For the W-2 phishing related breaches, total amounts claimed per class member averaged around \$2.75 per class member.⁴

This is, of course, a function of claims rates, as class members are not submitting claims for \$1.00. Rather, claims are necessarily only submitted by those who have been impacted—either by experiencing fraud or, at minimum, reacting to the potential of such fraud by monitoring accounts, changing their payment cards, freezing credit lines, etc. However, such limited claims rates are not unexpected. According to *The Aftermath of a Data Breach: Consumer Settlement (April 2014)*, sponsored by Experian Data Breach Resolution and conducted and reported by the Ponemon Institute, 81% of data breach victim respondents did not have any out-of-pocket expenses, and 55% of respondents reported taking no steps to protect themselves and their family from identity theft in the wake of a breach.⁵

Accordingly, resolutions like the proposed Settlement provide compensation targeted at those who need it; Class Members that experienced fraud or reacted to monitor and/or prevent it.

⁴ These averages were derived by dividing the total amount of valid funds claimed by the total class size.

⁵ Ponemon Institute LLC, *The Aftermath of a Data Breach: Consumer Settlement* (April 2014), p.7, available at <https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf>

D. The Court's Other Concerns

At the hearing the Court also referenced that the proposed Claim Form was potentially too long or confusing, especially considering the amounts at issue. To address the Court's concerns, the Parties worked together to streamline the proposed Claim Form, which is now just two pages long, as opposed to the prior version that was six pages long. The new proposed Amended Claim Form is attached hereto as **Exhibit 1**.

Likewise, to the extent the Court had any lingering concerns about the arm's length nature of the negotiations in this matter, the preparedness of counsel given the procedural posture of the case, or the zealousness of the advocacy on either Party's part, also attached hereto as **Exhibit 2**, is a declaration from Mediator Bennett Picker. Therein, Mr. Picker details the Parties' submissions and meetings with him, the arm's length nature of the negotiations, that "the lawyers with whom [he] met zealously represented the interests of their clients," and that he "was impressed by the quality of advocacy of counsel on both sides and can attest that there was a significant amount of work that went into reaching the result that was achieved in this case for the benefit of Plaintiff and the class." *Id.* at ¶¶ 11–12.

II. CONCLUSION

Based on their experience in analogous data breach cases, the Parties believe the proposed Settlement is a fair, reasonable, and adequate outcome for the Settlement Class. The Settlement relief fits closely with precisely the harms and concerns alleged in the Complaint: out-of-pocket costs, lost time, and protection of customer data going forward. Moreover, the Settlement structure is aimed at providing compensation to those impacted by the data breach; those who either experienced fraud or took action to monitor or prevent it. Importantly, based on counsel's

experience with (and review of) similar data breach cases, they believe that the amounts made available for claims will be sufficient.

Dated: April 27, 2020

Respectfully submitted,

/s/ Charles Schaffer

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663
cschaffer@lfsblaw.com

MORGAN & MORGAN

Patrick A. Barthle (*pro hac vice forthcoming*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
pbarthle@ForThePeople.com

Counsel for Plaintiff and the Proposed Settlement Class

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that on April 27, 2020, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

/s/ Charles Schaffer

Charles E. Schaffer

Exhibit 1

FIVE BELOW SECURITY INCIDENT SETTLEMENT CLAIM FORM

This Claim Form should be filled out and submitted by mail if you received notice that your credit or debit card was potentially compromised when you made an online purchase from Five Below in late 2018/early 2019. You may get a payment up to \$250 if you fill out this Claim Form. Please refer to the Settlement Notice posted on the settlement website, www.fivebelowcardsettlement.com, for more information. You may also fill out and submit a claim form on the settlement website by following the prompts.

First, please provide us your information so we may contact you.

First: _____ M: _____ Last: _____

Address: _____

City: _____ State: _____ ZIP: _____ Country: _____

Phone: _____ Email (*Optional*): _____

Second, please provide the password and username that the settlement administrator provided to you in the letter or email notifying you of the settlement. If you do not have this information but believe you may be a class member, please contact the settlement administrator at 1-866-742-4955.

Username: _____ Password: _____

Third, please describe your claimed damages. Three types of damages are available. First, you may recover certain out-of-pocket expenses incurred as a result of the Five Below Security Incident. Second, you may recover money to compensate you for time you spent addressing the incident. And third, you may receive a \$22 payment if you had a fraudulent charge on your card, even if those charges were reversed or repaid. These expenses or time must have been incurred during the applicable time period, which is generally from the security incident through the end of the claim deadline. Please refer to the Settlement Notice for more information.

1. Out-of-pocket expenses.

The types of expenses that you may claim include fees or other charges (e.g., interest, overdraft fees, etc.) from your bank or credit card company due to fraudulent activity on your card, any fee you paid to have a card reissued, expenses you incurred because your account was frozen for a period of time, and other incidental expenses (e.g., postage, long distance charges) you incurred addressing the Five Below Security Incident. The Settlement Notice describes the types of available expenses in greater detail. Please refer to that document for more information.

Documentation is required for claimed expenses. Please be sure to include documentation to expedite the processing of your claim.

Date	Description	Amount

Documentation: Attach supporting documentation. For example, a bank statement showing claimed fees (you may redact unrelated transactions and all but the first and last four digits of any account number).

2. Time spent addressing the security incident.

If you incurred a fraudulent charge on the affected payment card, you may receive reimbursement for up to five hours of time spent dealing with replacement card issues or in reversing fraudulent charges that occurred as a

Questions? Call _____ or visit www.fivebelowcardsettlement.com

result of the Five Below Security Incident (round to the nearest hour). You must submit documentation reflecting the fraudulent charge. If you did not incur a fraudulent charge, or do not have documentation, you may receive reimbursement for up to three hours of time by describing what you did. Time is paid at a rate of \$20 per hour.

To expedite the processing of your claim, please answer the following questions as specifically as possible:

How much time did you spend? 1 Hour 2 Hours 3 Hours 4 Hours 5 Hours

What did you do?

When, approximately, did this occur?

Documentation: If you claim more than three hours, you must attach documentation showing one or more fraudulent charges were posted to your account that you believe were caused by the Five Below Security Incident (you may redact as described above).

3. Payment for fraudulent charges.

If you had fraudulent charges to a credit or debit card account (even if they were reversed or repaid), you are eligible to claim a \$22 cash payment for each card. Documentation reflecting the charges is required.

First four and last four digits of card	Date of charges (only 1 per card required)

Documentation: For each card, provide a statement or other documentation showing a fraudulent charge(s) was posted to your account that you believe were caused by the Five Below Security Incident (you may redact as described above).

Last, you must certify that the information you provided above is true and accurate. Please sign the following:

I declare under penalty of perjury under the laws of the United States and the State of _____ that the information supplied in this Claim Form by the undersigned is true and correct to the best of my recollection. I understand that I may be asked to provide supplemental information by the Settlement Administrator or Claims Referee before my claim will be considered complete and valid.

Print Name: _____

Signature: _____ Date: _____

* * *

Once complete, please mail this Claim Form and all required supporting documentation to the following address, postmarked by _____, 2020:

Five Below Security Incident Settlement
 c/o RG/2 Claims Administration LLC,
 P.O. Box 59479
 Philadelphia, PA 19102-9579

Questions? Call _____ or visit www.fivebelowcardsettlement.com

Exhibit 2

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

Marie Abdelmessih, individually and on behalf of all others similarly situated,)	
)	Case No. 2:19-cv-1487-JP
Plaintiff,)	
)	Judge John R. Padova
v.)	
)	
Five Below, Inc.,)	
)	
Defendant.)	

DECLARATION OF BENNETT G. PICKER

I, Bennett G. Picker, declare as follows:

1. I am Senior Counsel at the law firm of Stradley Ronon Stevens & Young, LLP in Philadelphia, Pennsylvania. I have personal knowledge of the information described in this declaration, and if called as a witness could and would testify competently about it. I am providing this declaration to describe for the Court the process by which agreement was reached on both the settlement and attorneys' fees. All parties expressly reserve the mediation and other applicable privileges.
2. I have been a full-time mediator for 14 years. I have over 30 years of experience mediating complex business disputes, including numerous class actions and data breach cases.
3. Last fall, I was selected by counsel for the parties to serve as the mediator for this case. The mediation was scheduled for November 22, 2019.
4. Prior to the in-person mediation session, the parties submitted confidential mediation briefs to me. Based on these submissions, as well as a review of the Plaintiff's complaint and Defendant's motion to dismiss, I learned that the case presented significant risks to both sides.

5. I also learned that the parties had been engaged in settlement discussions prior to my engagement, including a written demand letter and a response. This correspondence was forwarded to me in preparation for the mediation.

6. On November 6 and 20, in advance of the mediation session, I held telephone conferences with counsel to discuss the mediation structure, the parties' confidential submissions, as well as the parties' positions on a possible class-wide resolution.

7. At the November 22 mediation session, two Five Below representatives attended in person.

8. After several rounds, the parties agreed upon the settlement terms that were subsequently presented to the Court. These terms were negotiated extensively during the mediation.

9. In addition, Five Below agreed to provide Plaintiff confirmation that several information security tasks had been or would be completed at the company. This was also the subject of significant negotiation.

10. The parties did not discuss attorneys' fees, litigation expenses, or incentive awards until after the material substantive terms of the settlement had been agreed upon. After significant negotiation, the parties finally reached an agreement on the amount of Plaintiff's attorneys fees and expenses, subject to Court approval. The parties also agreed on the service award payment amounts to the class representative, which is likewise subject to Court approval.

11. At all times, these negotiations were conducted at arm's length and in good faith. At all times, the lawyers with whom I met zealously represented the interests of their clients.

12. I was impressed by the quality of advocacy of counsel on both sides and can attest that there was a significant amount of work on the part of all counsel in the case that went into the result that was ultimately achieved.

I declare pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on April 16, 2020

By: /s/Bennett G. Picker
Bennett G. Picker (PA Bar ID No. 13300)
Stradley Ronon Stevens & Young, LLP
2005 Market Street, Suite 2600
Philadelphia, PA 19103
Tel: (215) 564-8054
Email: bpicker@stradley.com