

EXHIBIT 1

Supplemental Declaration from Class Counsel

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

In re: Equifax Inc. Customer
Data Security Breach Litigation

MDL Docket No. 2800
No. 1:17-md-2800-TWT

CONSUMER ACTIONS

Chief Judge Thomas W. Thrash, Jr.

**CLASS COUNSEL'S SUPPLEMENTAL DECLARATION IN SUPPORT
OF PLAINTIFFS' MOTION FOR ATTORNEYS' FEES, EXPENSES, AND
SERVICE AWARDS TO THE CLASS REPRESENTATIVES**

Kenneth S. Canfield, Amy E. Keller, and Norman E. Siegel declare as follows:

1. We were appointed by this Court to serve as Co-Lead Counsel for the Consumer Plaintiffs and Interim Class Counsel in the above-captioned MDL. Along with Roy E. Barnes, who serves as Co-Liaison Counsel with lead responsibilities, we have led the Plaintiffs' efforts in the consumer track since our appointment on February 9, 2018. We make this Declaration in support of Plaintiffs' motion for attorneys' fees, expenses, and service awards to the class representatives. We have personal knowledge of all the matters addressed in this Declaration.

2. This Declaration supplements our declaration submitted as part of Plaintiffs' Motion to Direct Notice of Proposed Settlement to the Class [Doc. 739-

4], which provided the Court with a history of the litigation, described Class Counsel's work leading up to the filing of that motion, and otherwise addressed facts that were relevant to the Court's decision whether to direct notice to the class.

3. This Declaration focuses on the facts that bear on the Court's determination of a reasonable fee in connection with Plaintiffs' fee application and, among other things, summarizes our work in litigating and settling this matter, our continued work on behalf of the proposed settlement class since this Court ordered issuance of notice, and our years of anticipated future work sponsoring and administering the settlement. Because some of the same facts relate to both the motion to direct notice and our fee application and for ease of reference, we have reiterated here some of the same facts that we covered earlier. This Declaration also summarizes the timekeeping protocols we developed and applied to all counsel, our efforts to efficiently allocate work, and the lodestar incurred in performing that work. Finally, this Declaration addresses Plaintiffs' requests for reimbursement of reasonable expenses and modest service awards to the class representatives.

Class Counsel's Work on Legal and Discovery Matters

4. On September 7, 2017, Equifax announced that criminals had stolen from its computer networks confidential personal and financial information pertaining to millions of consumers and eventually admitted that about 147 million Americans were impacted. Class action lawsuits against Equifax immediately began to be filed by affected consumers and financial institutions. Ultimately, more than 300 such lawsuits were filed around the country.

5. In December 2017, the Judicial Panel on Multidistrict Litigation transferred these lawsuits to this Court. The Court created two separate tracks to manage the litigation – one for the consumer cases and one for the cases brought by financial institutions. On February 12, 2018, the Court appointed a group of 13 lawyers to lead the litigation including Ken Canfield, Amy Keller, and Norman Siegel as Co-Lead Counsel and Roy Barnes as Co-Liaison Counsel, sharing duties with Co-Lead Counsel. [Doc. 232] This group was also appointed Interim Consumer Class Counsel pursuant to Fed. R. Civ. P. 23(g), and referred to as “Class Counsel” in the Settlement Agreement and this Declaration. The legal team appointed to lead the consumer track includes some of the nation’s most respected class action lawyers who collectively have prosecuted over 50 data breach cases, including all of the most significant cases brought both before and after this MDL.

6. As Class Counsel, our first major task was to file a consolidated amended complaint, which the Court had announced would serve as the vehicle for litigating the consumer claims. Our group had a substantial head start on this task because prior to our appointment we had already filed a case that named class representatives from every state. Nonetheless, the consolidated complaint was a massive undertaking, involving investigating the underlying facts, vetting several thousand potential class representatives, and thoroughly researching many legal theories under federal law and the laws of all 50 states. On May 14, 2018, Plaintiffs filed our 559-page consolidated amended consumer complaint, which named 96 class representatives and asserted numerous common law and statutory claims under both state and federal law. [Doc. 374]

7. In June 2018, Equifax moved to dismiss the complaint in its entirety. [Doc. 425] Equifax's primary focus was attacking Plaintiffs' negligence and negligence per se claims, arguing that Georgia law does not recognize a legal duty to safeguard personal information, none of the class representatives (or any class members) suffered a legally-cognizable injury, and Plaintiffs could not plausibly prove any alleged injury was caused by the Equifax data breach. The motion to dismiss was exhaustively briefed during the summer and early fall of 2018. [Docs. 452, 464, 483] On December 14, 2018, the Court heard more than three hours of oral

argument on Equifax's motion to dismiss. [Doc. 534] Then, on January 28, 2019, the Court largely denied Equifax's motion. [Doc. 540] Equifax answered on February 25, 2019. [Doc. 571]

8. While the consolidated amended complaint was being prepared and Equifax's motion to dismiss was pending, Class Counsel and the members of the Plaintiffs' Steering Committee undertook a substantial amount of additional work to move the case forward. That work included the organizational activity that is part of leading any case of this magnitude (establishing committees, assigning areas of responsibility, hiring vendors for e-discovery, etc.), as well as tasks such as locating and consulting with experts; working with the class representatives to assemble their documents and compile their damages; investigating the facts relating to the breach, including the mechanism for how the breach occurred and the data was exfiltrated; communicating with public interest groups active in the cybersecurity, consumer protection, and financial fraud fields; coordinating with the leadership of the financial institution track and the related securities litigation; developing our strategy for prosecuting the case; meeting with state and federal lawmakers regarding the breach; issuing document retention subpoenas to scores of third parties; and attending monthly status conferences in court.

9. Under the local rules of the Northern District of Georgia, discovery does not begin until 30 days after an answer is filed. Nevertheless, we were able to secure case management orders that front-loaded much of the preparatory work needed before formal discovery could as a practical matter proceed and set the groundwork for discovery once the motions were decided. In accordance with these orders, the parties negotiated a series of protocols to govern discovery, exchanged requests for production of documents, and attempted to negotiate the search terms and list of custodians that would be used in electronic searches. [Doc. 258] (Protective Order); [Doc. 449] (Production and ESI Protocol) Several parts of this pre-discovery process proved to be challenging, forcing Class Counsel to spend substantial time on these matters. On some issues, the parties reached impasse compelling Class Counsel to file a motion seeking limited relief from the discovery stay and an order facilitating our interviews of former Equifax employees who had signed non-disclosure agreements. [Doc. 488]

10. Once the Court ruled on Equifax's motion to dismiss, formal discovery commenced, and Plaintiffs' efforts intensified. Among other things, Class Counsel and the Plaintiffs' Steering Committee reviewed over 500,000 pages of documents produced by Equifax, as well as many thousands of native files including presentations and databases; began producing named plaintiffs' documents to

Equifax; and scheduled depositions of several former Equifax employees. Our document review was complicated by Equifax's decision to segregate additional, allegedly highly-confidential documents in a "reading room" controlled by Equifax, which involved beginning to negotiate revised orders concerning discovery and creating new review protocols, along with meeting and conferring about Equifax's ongoing productions. Those efforts continued up to the moment the case settled.

11. Class Counsel fought to protect the consumer class's interests on multiple fronts. For example, this Court had already answered in the affirmative the question of whether Equifax had a legal duty to protect Plaintiffs' personal data. But this important question, among others, was being actively litigated in the Georgia appellate courts during the pendency of this case. In fact, Class Counsel drafted and filed before the Georgia Supreme Court an amicus brief regarding the scope of the negligence duty to protect confidential personal information in *Georgia Department of Labor v. McConnell*, attached hereto as Exhibit A. We filed the brief so that the Supreme Court would be fully informed of the facts relating to this case and the potential implications of its ruling for the class.

Overview of Settlement Discussions

12. Settlement discussions began in September 2017. After initial telephone and in-person discussions regarding a potential settlement process, the

parties retained Layn R. Phillips, a former federal judge and principal of Phillips ADR, to serve as mediator. Judge Phillips is perhaps the country's preeminent mediator in major civil litigation and has successfully mediated several other data breach cases, including *In re Anthem Customer Data Breach Security Litig.*, which until now is the most successful consumer data breach settlement. Our first negotiating session took place in Newport Beach, California on November 27-28, 2017. The parties engaged in extensive preparation for the mediation and exchanged comprehensive mediation statements.

13. Although little progress was made at the first mediation, it did serve to initiate what became a lengthy back-and-forth process with Equifax that lasted over the next 16 months. The parties negotiated over this period with the oversight of Judge Phillips – work that involved exchanging additional mediation statements, numerous and regular telephone conferences, and additional all-day mediation sessions with Judge Phillips on May 25, 2018, August 9, 2018, November 16, 2018, and March 30, 2019. During this period, Class Counsel and the Plaintiffs' settlement committee also spent significant time with vendors so that we could develop and deliver state-of-the-art monitoring and restoration services to the entire class. We also retained several leading cybersecurity experts to assist us and consulted with

knowledgeable consumer groups and dozens of consumer advocates, Congressional staff, and state Attorneys General.

14. The technical changes needed to secure Equifax's data security system presented a difficult issue. And once the cause of the breach was determined, how to ensure that Equifax properly fixed its vulnerabilities presented another important challenge. It was critical that the technical changes would not only force Equifax to adopt measures to decrease the likelihood of a future breach, but also to ensure that its systems were designed so as to minimize the impact if another breach does occur. This was a particularly important component of the negotiations because unlike most data breach victims, the class here did not choose to do business with Equifax and cannot prevent Equifax from continuing to store their sensitive personal information. The parties worked on detailed and comprehensive business practice changes involving Equifax's cybersecurity measures. In connection with the negotiations, we retained Mary Frantz, one of the nation's leading cybersecurity experts. Working with Ms. Frantz, we examined Equifax's existing data security systems, attended meetings including at Equifax's headquarters in Atlanta with Equifax's counsel and its security experts to discuss the cause of the breach and Equifax's remedial efforts, and exchanged numerous proposals and counter-proposals before reaching an agreement in March 2019 (as addressed below).

15. Although the negotiations were productive and moved the parties closer to settlement, the process slowed substantially following the November 16, 2018 mediation session, and eventually came to a stop in December. From Class Counsel's perspective, Equifax would not meet Plaintiffs' demands unless and until Plaintiffs successfully navigated the case past the motion to dismiss. It was only after the Court entered its lengthy order largely denying Equifax's motion to dismiss that negotiations resumed in February 2019. Judge Phillips convened what proved to be the final mediation on March 30, 2019. After getting consensus on all terms other than the size of the fund (including the individual relief and extensive business practice changes), the parties reached impasse. Late in the evening, Judge Phillips made a "mediator's proposal," which both sides accepted, and the parties executed a binding Term Sheet at about 11 p.m., subject to approval by Equifax's board of directors, which occurred the next day. A copy of the binding March 30 Term Sheet is attached hereto as Exhibit B.¹

16. From the outset of the negotiations, Class Counsel had focused on three major components of relief. First, the establishment of a cash settlement fund to

¹ Exhibit A to the Term Sheet includes proprietary information supplied by the monitoring vendor and is therefore not included in this attachment. The elements of the monitoring services were explained in detail in Exhibit 4 to the Settlement Agreement.

compensate those class members that had suffered out-of-pocket losses and lost time as a result of the breach. Second, the provision of high-quality credit monitoring and identity restoration services specifically tailored to address the data compromised in this breach. And third, modifications to Equifax’s data security practices that would be subject to Court enforcement, which would protect the class—most of whom have no relationship with Equifax—well into the future. The March 30, 2019 Term Sheet achieved all of these goals, as further specified in Class Counsel’s Declaration in Support of Motion to Direct Notice. (*See* Doc. 739-4, ¶¶ 27-31)

Input from Federal and State Regulators

17. The binding Term Sheet reached on March 30, 2019, provided for a period of 60 days for Equifax to share the Term Sheet with, and for Class Counsel to consider any comments from, the Federal Trade Commission, the Consumer Financial Protection Bureau, and state Attorneys General (“Regulators”) regarding the relief afforded to the class. This provision is consistent with guidance provided by the Federal Judicial Center regarding solicitation of the views of federal and state regulators regarding class action settlements. *See generally*, Federal Judicial Center, *Managing Class Action Litigation: A Pocket Guide for Judges* at 26-27. Because the Regulators were not involved in negotiating the Term Sheet, the parties agreed that, “to the extent that the Regulators propose changes to the class benefits or the Term

Sheet, Plaintiffs will discuss and consider in good faith such changes, and if the parties agree, the Term Sheet and settlement agreement will be amended accordingly.” (Ex. B, § VII). The parties agreed that if Class Counsel or Equifax rejected those changes, the Term Sheet would be enforced as the final settlement.

18. In the weeks that followed, the Regulators proposed substantive changes to the Term Sheet. Many of the proposed changes were minor, while others provided more substantial relief, including increasing the settlement fund from \$310 million to \$380.5 million. Class Counsel supported the changes that benefitted members of the settlement class, but opposed others that might diminish the relief available under the Term Sheet or otherwise make class members worse off. Class Counsel’s opposition to some of the individual proposals triggered another round of difficult and intense negotiations that lasted over two months, but ultimately the issues were successfully resolved when Equifax and the Regulators agreed to modifications that ensured that class members would only benefit from changes made to the March 30, 2019 Term Sheet. On July 19, 2019, Equifax and Plaintiffs executed the Settlement Agreement. Plaintiffs submitted the agreement and moved for an order directing notice to the class on July 22. The same day, after a hearing, the Court granted the motion, authoring issuance of notice to the class. [Doc. 742]

19. After Plaintiffs and Equifax finalized the settlement agreement,

Equifax entered into separate settlements with the Regulators. The regulatory settlements expressly refer to and are dependent upon the class action settlement Class Counsel negotiated, incorporate its substantive terms, and rely upon and defer to the class action settlement to distribute all relief to impacted consumers. Accordingly, this is not a case where Class Counsel piggybacked on the effort of government regulators to achieve a private settlement. To the contrary, Class Counsel negotiated a binding settlement with Equifax without the involvement or assistance of the Regulators. While Class Counsel later agreed to modify the settlement to provide additional relief that the Regulators initiated, incorporating the additional relief into the settlement was a difficult and lengthy process, and was finally brought to fruition through Class Counsel's extensive efforts.

20. During the period from March 30, 2019 until mid-July, 2019, in addition to negotiating with Equifax and the Regulators regarding the scope of the relief in the settlement agreement, we spent considerable time first selecting and then working with Signal Interactive to craft what we believe is a state of the art notice program; and successfully convincing Equifax to agree to the program. We also consulted with federal and state regulators, who provided input. The process was laborious. The parties discussed the details of every email, social media advertisement, video, newspaper and radio advertisement to which the class would

be exposed, ranging from their substantive content and headlines to such matters as the facial expressions of the actors featured in the advertisements. The parties also negotiated about the scripts that would be used during the focus groups Signal has conducted, the questions that were included in the public opinion survey, and issues relating to many other topics. Simultaneously, we selected and worked with JND to design a settlement website allowing class members to file electronic claims; drafted a claims protocol that covered every step of the claims process from filing through verification and adjudication of electronic claims; prepared the scripts for hundreds of telephone operators to use in responding to questions from class members; and otherwise managed development of the claims and administration process. During this time, we traveled to JND's headquarters in Seattle to tour their facility, observe their operations, and meet with their senior management. We also spent considerable time negotiating and coordinating with Equifax and the Regulators regarding the claims and administration process to reach agreement on the final documents, forms, notices, and procedures that would be used.

Class Counsel's Work After the Order Authorizing Class Notice

21. On the morning of July 22, 2019, before Class Counsel had presented the settlement to this Court and the official notice program had been authorized to begin, there was a deluge of pervasive and in some respects misleading coverage in

the national media following regulators' statements and press conferences announcing their separate settlements with Equifax. The media coverage created a widespread misperception that all consumers impacted by the data breach (and in some cases all Americans, regardless of class membership) could get alternative compensation of \$125 simply by filing a claim.

22. Under the settlement, not everyone is eligible for alternative compensation and even those eligible are not guaranteed \$125. The settlement limits alternative compensation to those who already have credit monitoring services, do not want the services available under the settlement, attest they will maintain their own service for at least six months, and provide the name of their current provider. Moreover, the settlement provides that alternative compensation claimants will receive *up to* \$125, not a \$125 guaranty. The amount available to pay alternative compensation claims is capped at \$31 million to ensure there are sufficient funds to pay for credit monitoring, out-of-pocket losses, and other benefits. If the cap is exceeded during the initial claims period, alternative compensation claims will be reduced and paid pro rata. The cap will be lifted at the end of the extended claims period if money remains after other benefits are paid. [Doc. 739-2, ¶ 7.5]

23. The settlement website went live on the evening of July 23, 2019, allowing consumers to find out if they were class members and file electronic claims

for benefits. Less than 48 hours later, and prior to the issuance of the Court-approved notice, Class Counsel learned that millions of claims already had been filed, most of which sought alternative compensation rather than credit monitoring. While Class Counsel suspected many of these claims might be invalid, it seemed likely given the erroneous and pervasive press coverage around the \$125 claim that the \$31 million cap would be reached and thus alternative compensation claimants would receive substantially less than \$125.

24. Class Counsel immediately contacted defense counsel and proposed adjustments to the notice and claims program to directly address the erroneous and misleading coverage of the settlement in the media so that class members would be adequately informed about the situation and those who had already filed claims would be given a chance to file an amended claim to change the type of relief they preferred under the settlement. When issues remained after Class Counsel's negotiation with Equifax regarding this proposed corrective action, Class Counsel sought emergency relief from the Court. At a hearing on July 30, 2019, the Court approved Plaintiffs' proposals, which were implemented. Further, Class Counsel issued a public statement on August 1, 2019, explaining the terms of the settlement and urging class members to rely only on the official notice authorized by this Court, not the media or other sources. *See Exhibit C.*

25. Since the Court's order authorizing class notice, Class Counsel have also spent substantial time on other matters, such as overseeing implementation of the claims and notice programs; communicating with JND, Signal, defense counsel, and the Regulators (including through weekly conference calls); answering hundreds of questions from class members; evaluating and responding to objections; and working on the papers that will be filed before the final approval hearing.

Class Counsel's Substantial Anticipated Work Over the Coming Years

26. Class Counsel's work will not end once the settlement is finally approved or even after all appeals are resolved. Class Counsel's oversight responsibilities and other work will continue until the settlement is finally consummated, which will not occur until far into the future. The initial claims period does not end until January 2020, and will be followed by a four-year extended claims period. Identity restoration services will be available to class members for three more years after that. The notice program will continue throughout this entire seven-year period. Moreover, as the settlement administrator begins verifying claims, Class Counsel will be hard at work monitoring the process and where necessary participating in the dispute resolution procedures as contemplated by the claims protocol. (Ex. 9 to Settlement Agreement, Doc. 739-2 at 285-292). As further set forth below, Class Counsel anticipate spending an additional 10,000 hours of lawyer

time on behalf of the settlement class, after the entry of final approval.

Class Counsel's Request for a Percentage of the Common Fund

27. Class Counsel successfully negotiated the largest data breach settlement in history. The \$380.5 million fund alone is more than the combined total recovered—roughly \$350 million—in all of the significant data breach settlements over the last ten years. (See Doc. 739-4 at 40-45) Further, class members are eligible for substantial individual benefits that are equivalent to or vastly exceed those available in prior settlements.

28. The requested fee of \$77.5 million is 5.6 percent of the *minimum* \$1.38 billion Equifax has committed to this settlement and 20.368 percent of the \$380.5 million cash settlement fund. The requested fee was derived from the settlement Class Counsel negotiated before the Regulators' involvement. In the Term Sheet, Class Counsel agreed to seek 25 percent of the initial \$310 million fund, or \$77.5 million. (Ex. B, § IV) This fee was not discussed until after the parties had agreed on relief to the class.

29. In the modified settlement, Class Counsel agreed to the same fee, [Doc. 739-2 at 25-26], deciding to forego additional compensation for the substantial work we performed and the class benefits that were secured after the Regulators became involved. We believe we would have been entitled to a larger fee but for our decision.

This MDL litigation, and Class Counsel's groundbreaking work leading to the March 30 Term Sheet, paved the way for this final settlement. Thus, while the Regulators were the catalyst for increasing the fund for example, Class Counsel played a crucial role integrating the additional money into the settlement to benefit the class.

30. Although the requested fee can be measured as 20.368 percent of the \$380.5 million cash settlement fund or 5.6 percent of the minimum \$1.38 billion Equifax has committed to this settlement, these percentages do not reflect the true value of the benefits available to class members. For example, the opportunity to claim free credit monitoring is a concrete benefit for all 147 million class members, without any limits or caps. The cost for the first seven million will be paid out of the \$380.5 million fund; if more than seven million sign up, Equifax must pay for these services outside of the fund. Based on the declaration of James Van Dyke, our discussions with other experts, and publicly-available pricing, the value of this benefit is at least \$1,920 for each class member and more than \$282 billion for the entire class. While all class members will not file a credit monitoring claim, nearly 3 million class members already have done so, claiming services worth nearly \$6 billion. The requested fee is therefore about 1.2 percent of the value of the claims

that already have been filed plus the cash fund and less than .027 percent of the retail value of the credit monitoring offered to the entire class.

31. The value also does not account for another benefit negotiated by Class Counsel to provide Settlement Class Members who enrolled in TrustedID Premier monitoring provided by Equifax following the data breach with an additional one-year of credit monitoring services (known as IDNotify) to allow for continuity of credit monitoring services while the settlement is being finalized. And it does not account for the value of the settlement provision prohibiting Equifax from imposing arbitration clauses under certain circumstances.

32. This case presented a host of novel and difficult legal questions, including whether Equifax had a duty to protect Plaintiffs' personal data and whether Plaintiffs' alleged injuries are legally cognizable and were proximately caused by the Equifax breach. The duty and injury questions were being actively litigated in the Georgia appellate courts during the pendency of this case. For example, in the *McConnell* case, the Georgia Court of Appeals held that under Georgia law there is no duty to safeguard personal information and its opinion was followed by years of additional appellate litigation. *See McConnell v. Dep't of Labor*, 787 S.E.2d 794, 797 & n.4 (Ga. Ct. App. 2016), *vacated on other grounds*, 805 S.E.2d 79 (Ga. 2017), *aff'd in part & rev'd in part on other grounds*, 814 S.E.2d 790, 799 (Ga. Ct. App.

2018). At the time Class Counsel entered into the Term Sheet, the case was before the Georgia Supreme Court on *certiorari*. After the settlement, the Georgia Supreme Court affirmed the Court of Appeals' decision on the duty issue. *See Dept. of Labor v. McConnell*, 828 S.E.2d 352 (Ga. 2019). Similarly, during the pendency of this litigation, in *Collins v. Athens Orthopedic Clinic*, 815 SE.2d 639, 644 (Ga. Ct. App. 2018), the Georgia Court of Appeals held that the fact of compromised data is not a compensable injury by itself in the absence of some loss or damage. At the time we entered into the March 30 Term Sheet, a *certiorari* petition was pending in the Georgia Supreme Court and was subsequently granted. To date, to our knowledge, the Georgia Supreme Court has not issued an opinion.

33. Other novel and difficult questions resulted from the sheer size of the litigation, the number of Americans impacted by the breach, and the highly technical nature of the facts. For example, determining and proving the cause of the breach and developing the cybersecurity measures needed to prevent a recurrence were particularly challenging. The settlement process that took place after the March 30 Term Sheet also raised numerous novel and difficult questions that increased the complexity of the settlement.

34. While the claims process is not yet complete, Class Counsel expect that class members who file valid claims for out-of-pocket losses will be paid in full with

no *pro-rata* reduction; as noted above, it appears that at least 3 million will claim credit monitoring collectively worth nearly \$6 billion; and class members who file claims for alternative compensation and time will be paid more than \$60 million. Moreover, all class members are entitled to identity restoration services for seven years regardless of whether they make a claim.

35. Had Class Counsel not taken on this case, we would have been able to spend significant time on other matters. Indeed, for many months, this case was all consuming. Because of the complexity and novelty of the issues involved, much of the work was performed by attorneys with the most experience on the Plaintiffs' team. Nearly every issue was case-dispositive, limiting Class Counsel from allocating substantial time to other matters. Thus, unlike some cases where it is appropriate to allocate substantial work to less experienced associates (or contract lawyers) this case demanded the full attention of Class Counsel and members of the Plaintiffs' Steering Committee.

36. Complex civil litigation customarily is handled on a contingent fee because consumers are unwilling and unable to pay substantial hourly rate fees and the potential recovery does not justify the economic investment. Contingent fees in such cases typically range from one-third to 40 percent of the recovery. The

requested fee is substantially below that range, and those charged by Class Counsel when negotiating contingency fees with private litigants.

37. This action was prosecuted entirely on a contingent basis. If Class Counsel had not achieved a recovery, we would have received nothing and, in fact, suffered a substantial out-of-pocket loss for the expenses we incurred litigating this case.

38. Class Counsel's business model involves prosecuting a relatively small number of major class actions, going for some time without revenue, and relying on periodic fee awards to pay overhead, generate profits, and finance the millions of dollars needed to cover the out-of-pocket expenses of litigation.

39. The time pressures in this case were extraordinary. The time necessary to complete even basic tasks in the time frame provided was complicated because of the novelty and uncertainty of the legal issues, the size of the class, the highly technical matters at the core of the case, and other factors that contributed to the magnitude of the undertaking. For example, filing the 559-page consolidated amended complaint involved vetting thousands of potential class representatives, thoroughly investigating the facts, researching the relevant case law in the federal courts and all 50 states, and drafting 99 separate counts. Further, the lengthy and contentious nature of the settlement negotiations created added time pressures,

particularly after we negotiated the March 30 Term Sheet and had to work not only with Equifax but also with federal and state regulators to meet the applicable deadlines. During the post-March 30 period, we also had to design, negotiate, and prepare to implement the state-of-the-art notice and claims programs in a compressed time in order to meet the deadlines under the Term Sheet. Additionally, specific events occurred and issues arose during the litigation that had to be addressed immediately, causing us to drop other matters and concentrate our efforts for several days or even weeks. For these and other reasons, we and other members of the Plaintiffs' legal team routinely and by necessity worked intensely, under great time pressure, to achieve the settlement now before the Court.

Class Counsel's Time and Expense Protocol and Reporting

40. In its February 12, 2018 Order appointing consumer leadership [Doc. 232, at 10-11], the Court directed: "All counsel must keep a daily record of their time spent and expenses incurred in connection with this litigation, and must report on a monthly basis their expenses and hours worked to Co-Lead and Co-Liaison Counsel. . . . In order for their time and expenses to be compensable, those not serving in leadership positions must secure the express authorization of Co-Lead Counsel for any project or work undertaken in this litigation." Further, the Court ordered: "On a quarterly basis . . . Co-Lead and Co-Liaison Counsel shall submit to

the Court in camera reports reflecting hours billed in this matter by all Plaintiffs' counsel. Failure to maintain and submit records with sufficient descriptions of time spent and expenses incurred may be grounds for denying attorneys' fees and/or expenses" (*Id.* at 10)

41. Class Counsel complied with that Order, issuing a time and expense protocol including detailed requirements, guidelines, and deadlines, and requiring that each submitted report must be certified by an attorney in each firm attesting to the accuracy of the submissions. Throughout the litigation, Class Counsel have timely submitted to the Court for its *in camera* review quarterly reports that contained the time we received from all Plaintiffs' counsel, with the exception of one firm. That firm's recorded time was not submitted because it did not meet the basic mandates of the billing protocol and failed to provide sufficient descriptions of the firm's work as required under the Court's leadership order.

42. After execution of the Term Sheet and ultimately the final settlement agreement, between June 2019 and the filing of this Declaration, Class Counsel reviewed each detailed time and expense entry submitted by all timekeepers pursuant to the protocol. As of September 30, 2019,² all Plaintiffs' counsel submitted

² Class Counsel will update these figures in the December 5, 2019, filing in final support of the settlement.

time reflecting 34,284.8 hours on this litigation, documented in the quarterly reports filed *in camera* with the Court. Class Counsel personally reviewed more than 21,000 time entries and excluded 3,272.9 hours as duplicative, unauthorized, of insufficient benefit, or inconsistent with the billing protocol we established at the outset of the litigation. The reviewed and revised records will be submitted to the Court for *in camera* review pursuant to the February 12, 2018 Order. The value of the revised time (31,011.9 hours) is \$20,986,357.80, at a blended rate of \$676.72. A chart reflecting the reasonable hours worked and lodestar incurred on behalf of the class for each firm is attached hereto as Exhibit D. The time reported in Exhibit D is reasonable and justified in view of the issues, the complexity and importance of the case, the manner in which the case was defended, and the quality of the result.

43. This lodestar is calculated using current rates, which are reasonable and routinely approved by courts in other class actions. A chart reflecting the rates, titles, and as applicable years of licensing for all timekeepers with more than 50 hours, is attached hereto as Exhibit E. In addition to Class Counsel's own experience in hundreds of class actions and hourly engagements, the Declarations of R. Klonoff (Ex. 2 to fee motion, ¶¶ 98-103) and H. Daniel (Ex. 3 thereto, ¶¶ 13, 16) support the reasonableness of these rates.

44. In a case of this size and complexity, and involving nearly 100 named class representatives, numerous firms and timekeepers necessarily made important contributions to securing the result achieved on behalf of the settlement class. In our review of pre-appointment billing records (before February 12, 2018), Class Counsel generally limited potentially compensable time to that incurred while communicating with and vetting individual consumer plaintiffs, and to specific work performed to comply with Court directives after creation of the MDL but before appointment of consumer leadership. After appointment of Co-Lead Counsel and the Plaintiffs' Steering Committee, the approved work performed by non-appointed firms was generally limited to working with leadership in vetting individual class-member clients and further working with named Plaintiffs on the pleadings, discovery, and settlement. As such, the vast majority of post-appointment time was performed by Co-Lead Counsel and the Plaintiffs' Steering Committee.

45. While numerous timekeepers worked in specific limited roles as assigned by Class Counsel, the vast majority of the work was performed by a core group comprised of Class Counsel and other leadership firms working at our direction on subject-matter committees.

46. From the beginning, Class Counsel made a conscious and rigorous effort to allocate assigned work in the most efficient manner practicable, calling on

lawyers with specific expertise to assist in those areas where we could most efficiently move the case forward. For example, Class Counsel directed PSC member Ariana Tadler to lead the ESI and offensive discovery efforts given her expertise in the field. Ms. Tadler worked with Amy Keller, who directed third-party discovery and conducted the majority of the consumer track's meet and confer discussions with third parties regarding document preservation. We asked David Berger, a lawyer certified as an Information Privacy Technologist, to work with the technical experts to craft the business practice changes. Other PSC members, including Andrew Friedman and John Yanchunis, provided invaluable insight from their leadership of large data breach cases including *Anthem*, and *Yahoo!*. Barrett Vahle and Kenneth Canfield, along with J. Cameron Tribble, were the primary drafters and editors of the main pleadings and briefs. Mr. Vahle bore first-hand responsibility for implementing the time and expense protocol. James Pizzirusso and Steven Nathan of his firm took the lead in our defensive discovery efforts and communicating with the named class representatives. Norman Siegel chaired the team that conducted the settlement negotiations. And, as the Co-Lead Counsel appointed by the Court and charged with the responsibility for this important case, the three of us necessarily devoted our full attention to every aspect of this litigation, constantly communicating with each other to coordinate our efforts and those of the

entire team, ensure that the litigation was handled efficiently, and even more importantly zealously represent our clients to obtain the best possible results for the class.

47. As a result of our oversight and commitment to the litigation, a relatively small number of timekeepers working in close concert were able to prosecute this MDL and achieve the historic settlement now before the Court, with: (1) the four primary firms (Co-Leads and the Barnes Law Group) performing 54.0% of the total hours of work and 58.5% of the total lodestar; (2) the appointed leadership firms performing 93.1% of the total hours of work and 95.1% of the total lodestar; (3) the top 6 timekeepers, all at the four primary firms performing 37.5% of the total hours of work and 47.0% of the lodestar; (4) the top 20 timekeepers, all at firms appointed by the Court to consumer leadership, performing 65.8% of the total hours and 74.0% of the lodestar; and (5) non-leadership firms contributing important but relatively modest work totaling less than 7% of the hours and 5% of the lodestar.

48. The substantial work completed to date is far from the end. We estimate that following the final approval hearing, Plaintiffs' counsel will spend an additional 10,000 hours over the next seven years in connection with the final approval and consummation of the settlement, including overseeing and managing the notice and

claims process. We reasonably expect to spend at least 2,500 hours in connection with matters relating to final approval of the settlement, dealing with objectors, and handling the inevitable appeals. Further, if the four principal firms (the three Co-Leads and the Barnes Law Group) each spend only about an hour per week on average overseeing the notice and claims processes and communicating with the various stakeholders over the next seven years, that is an additional 1,500 hours. Finally, we will spend considerable time in the process of verifying and adjudicating claims submitted by class members during the initial and extended claims periods, which will involve working with the settlement administrator to ensure valid claims are properly paid, communicating with class members whose claims have been denied, dealing with appeals from claim denials, and otherwise overseeing and managing the process. Based on the claims that have been made to date, we anticipate that there will be a robust claims rate in this case. Millions of claims, in fact, have already been made. If we must engage with 1% of the expected claims as part of the claims review process, it is likely that we will spend 10,000 hours or even substantially more on claims review and adjudication alone.

49. Plaintiffs' lodestar of \$20,986,357.80 as of September 30, 2019, results in a multiplier of just over 3.69 to reach the requested percentage fee. The multiplier is even lower if Class Counsel's future hours as estimated above are included in the

cross-check calculation. At the blended rate of \$676.72, the value of the time we estimate we will spend after final approval is \$6,767,200. The total of our current and future time thus is \$27,753,557.80, reducing the total multiplier to 2.79. These figures will be updated in conjunction with Plaintiffs' motion for final approval.

Requested Reimbursement of Expenses

50. The settlement agreement authorizes reimbursement up to \$3 million in expenses Class Counsel reasonably incurred on behalf of the class. Class Counsel have reasonably and necessarily incurred \$1,248,033.46 in expenses for such items as court reporter fees; document and database reproduction and analysis; e-discovery costs; expert witness fees; travel for meetings and hearings; paying the mediator; and other customary expenditures. Supporting detail for each of these current expenses has been reviewed by Class Counsel. A chart summarizing these expenses by category is attached hereto as Exhibit F.

51. Class Counsel will present to the Court any additional compensable expenses incurred after September 30, 2019, in connection with our forthcoming motion for final approval and supporting papers.

Class Representative Service Awards

52. The settlement agreement provides for a modest service award of \$2,500 to each class representative, identified in Exhibit G hereto, who devoted

substantial time and effort to this litigation working with their lawyers to prosecute the claims and were instrumental in achieving a settlement benefitting the entire class. Each of these individuals provided detailed information of the circumstances regarding the impact of the breach that was vital to Class Counsel's investigation and litigation of the class's claims. Class representatives provided bank records, credit card statements, and in some instances information about frauds they experienced after the breach. Furthermore, each of them has remained active in the case, communicating with the attorneys working on the case during subsequent phases of the case including individualized discovery and settlement. But for the class representatives' service, other class members would have received nothing.

We declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed this 29th day of October, 2019.

/s/ Kenneth S. Canfield
Kenneth S. Canfield

/s/ Amy E. Keller
Amy E. Keller

/s/ Norman E. Siegel
Norman E. Siegel

EXHIBIT A

Class Counsel's Amicus Brief *Dept. of Labor v. McConnell*

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

IN THE SUPREME COURT FOR THE STATE OF GEORGIA

Case No. S18G1317	Case No. S18G1316
Thomas McConnell, et al., <i>Appellants,</i>	Georgia Department of Labor, <i>Appellant,</i>
v.	v.
Georgia Department of Labor, <i>Appellee.</i>	Thomas McConnell, et al., <i>Appellees.</i>

**AMICUS CURIAE BRIEF OF THE CONSUMER PLAINTIFFS IN THE
EQUIFAX DATA BREACH MULTI-DISTRICT LITIGATION**

Roy E. Barnes
Georgia Bar No. 039000
The Barnes Law Group, LLC
31 Atlanta Street, S.E.
Marietta, Georgia 30060
770-227-6375

Kenneth S. Canfield
Georgia Bar No. 107744
Doffermyre Shields Canfield &
Knowles LLC
1355 Peachtree Street, Suite 1725
Atlanta, Georgia 30309
404-881-8900

David J. Worley
Georgia Bar No. 776665
Evangelista Worley LLC
8100 A Roswell Road, Suite 100
Atlanta, Georgia 30350
404-205-8400

Counsel for Amici Curiae

TABLE OF CONTENTS

INTRODUCTION	1
INTEREST OF AMICUS CURIAE	2
FACTUAL BACKGROUND.....	4
A. Recent Criminal Data Breach Litigation.....	4
B. The Facts And Circumstances Relating To The Equifax Data Breach.....	6
ARGUMENT	11
A. The Facts And Circumstances In This Case Are Starkly Different Than In Criminal Data Breach Cases Such As <i>Equifax</i>	12
B. The Court Should Not Address The Merits Of A Negligence Claim In A Criminal Data Breach Case Based On The Record In This Case.	17
C. This Court Should Be Cautious About Potentially Restricting Claims Of Criminal Data Breach Victims Widely Allowed In Other Courts.....	19
CONCLUSION.....	21

TABLE OF AUTHORITIES

Cases

Amos v. City of Butler, 242 Ga. App. 505 (2000).....14

Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011)..... 20, 21

In re Anthem, Inc. Data Breach Litig.,
2016 WL 3029783 (N.D. Cal. May 27, 2016) 20, 21

In re Arby’s Rest. Grp. Inc. Litig.,
2018 WL 2128441 (N.D. Ga. Mar. 5, 2018)..... 5, 6, 15, 20

Banknorth, N.A. v. BJ’s Wholesale Club, Inc.,
394 F. Supp. 2d 283 (D. Me. 2005).....20

Brush v. Miami Beach Healthcare Grp. Ltd.,
238 F. Supp. 3d 1359 (S.D. Fla. 2017).....20

Chrysler Grp., LLC v. Walden, 303 Ga. 358 (2018)17

Clapper v. Amnesty Int’l USA, 568 U.S. 398 (2013).....21

Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018).....20

In re Equifax, Inc., Customer Data Security Breach Litig.,
2019 WL 937735 (N.D. Ga. Jan. 28, 2019) passim

In re Experian Data Breach Litig.,
2016 WL 7973595 (C.D. Cal. Dec. 29, 2016).....20

F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)13

Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333 (W.D.N.Y. 2018).....20

Galaria v. Nationwide Mut. Ins. Co., 663 F. App’x 384 (6th Cir. 2016).....15

Hapka v. CareCentrix, Inc., 2016 WL 7336407 (D. Kan. Dec. 19, 2016).....20

In re The Home Depot, Inc., Customer Data Security Breach Litig.,
2016 WL 2897520 (N.D. Ga. May 18, 2016)5, 6

Hutton v. Nat’l Bd. of Examiners in Optometry, Inc.,
892 F.3d 613 (4th Cir. 2018) 20, 21

Jones v. Commerce Bancorp, Inc.,
2006 WL 1409492 (S.D.N.Y. May 23, 2006)20

Lewert v. P.F. Chang’s China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016)20

Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.,
729 F.3d 421 (5th Cir. 2013)20

McConnell v. Department of Labor, 337 Ga. App. 457 (2016)17

McConnell v. Department of Labor, 345 Ga. App 669 (2018)..... 18, 19

Pennsylvania State Employees Credit Union v. Fifth Third Bank,
2006 WL 1724574 (M.D. Pa. Jun. 16, 2006)13

Pulte Home Corp. v. Simerly, 322 Ga. App. 699 (2006).....14

Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015) 15, 20, 21

Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012).....20

S. Indep. Bank v. Fred’s Inc.,
2016 WL 11164794 (M.D. Ala. Sept. 23, 2016).....20

Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739 (S.D.N.Y. 2017).....20

Savidge v. Pharm-Save, Inc., 2017 WL 5986972 (W.D. Ky. Dec. 1, 2017).....20

Smith v. Triad of Alabama, LLC,
2015 WL 5793318 (M.D. Ala. Sept. 29, 2015).....20

In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,
996 F. Supp. 2d 942 (S.D. Cal. 2014)20

In re Target Corp. Customer Data Sec. Breach Litig.,
64 F. Supp. 3d 1304 (D. Minn. 2014)20

Underwood v. Select Tire, Inc., 296 Ga. App. 805 (2009)14

Weinberg v. Advanced Data Processing, Inc.,
147 F. Supp. 3d 1359 (S.D. Fla. 2015).....20

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)..... 20, 21

Statutes

15 U.S.C. § 45.....5
O.C.G.A. § 10-1-393.8.....18
O.C.G.A. § 10-1-910.....18

INTRODUCTION

In September, 2017, Equifax, Inc., one of the nation’s three major credit reporting agencies, announced criminal hackers had accessed its networks and stolen sensitive personal information of nearly 150 million Americans. Resulting legal claims against Equifax – including more than three hundred class actions by consumers and financial institutions – are consolidated in a federal multi-district proceeding before Chief Judge Thomas Thrash of the U.S. District Court for the Northern District of Georgia. The consumer plaintiffs in that proceeding, through their court-appointed counsel, file this amicus brief to apprise the Court of the potential impact its ruling may have on their claims against Equifax. Amici take no position on the two legal issues upon which this Court granted certiorari, that is, whether Mr. McConnell’s claims are barred by sovereign immunity and whether his claims state a cause of action.

This appeal touches upon the duty and injury elements of a negligence claim arising from the disclosure of personal information. If the Court decides against Mr. McConnell and does so in perhaps unintentionally broad strokes (as the trial court may have done in flatly stating that in Georgia there is no duty to safeguard personal information), the rights of those victimized by the Equifax data breach could be restricted. Amici thus urge the Court to expressly limit its opinion to the facts and legal claims presented in this case, avoiding unintended consequences

that might occur if the opinion uses sweeping language that arguably could be extended to other situations in which confidential personal information is improperly disclosed or stolen.

Amici do so for three reasons. *First*, as the Department of Labor argues and two federal judges have specifically held, the circumstances in a criminal data breach case such as Equifax are starkly different. This case, as a result, is not a good vehicle for addressing those distinct circumstances. *Second*, issues relating to the duty and injury elements of a negligence claim in a criminal data breach case should only be decided based upon a fulsome factual record and fully-developed legal arguments, neither of which exist here. And, *third*, courts around the country routinely hold that the duty and injury elements are satisfied in a criminal data breach case, including three recent federal cases in Georgia. If this Court were to use language suggesting otherwise, Georgia would become a distinct outlier.

INTEREST OF AMICUS CURIAE

The consumer claims against Equifax in the multi-district litigation are being prosecuted by ninety-six individual plaintiffs from fifty states and the District of Columbia representing a proposed national class of all Americans whose personal information was stolen. They have brought claims for negligence, negligence *per se*, and various other legal theories. Each plaintiff, including all five Georgians, alleges injury. For example, after the breach, John Simmons of Acworth, Georgia

had unauthorized bank accounts opened in his name, causing his credit score to drop, delaying approval of a home loan, and requiring him to close the accounts, file police reports, and clean up his credit files. Other plaintiffs had unauthorized accounts opened in their names; had fraud losses; froze their credit reports and bought credit monitoring services to protect themselves as Equifax urged them to do; and otherwise spent time and money responding to the breach. All plaintiffs remain at substantial risk of future identity theft and fraud because their confidential information is in the hands of criminals.

The consumer plaintiffs are interested in this appeal because this Court's ruling may potentially impact their negligence-based claims against Equifax.¹ In seeking dismissal of those claims, Equifax argued unsuccessfully that the Court of Appeals' decision in this case stands for the proposition it has no legal duty under Georgia law to safeguard any of the confidential personal information it collects on virtually all Americans and that no plaintiff suffered a breach-related injury that is legally cognizable in Georgia. Amici expect Equifax may renew its arguments depending on the language used by this Court in resolving this appeal. This brief

¹ The plaintiffs are represented by a team of lawyers from around the country appointed by Judge Thrash to prosecute the claims in the multi-district litigation, including co-lead counsel Ken Canfield and co-liaison counsel, Roy Barnes and David Worley. Those attorneys are members of this Court's bar and sign this brief on behalf of the entire legal team pursuant to Rule 23 of this Court's rules.

is being filed to ensure that this Court is aware of the potential ramifications for the Equifax litigation of an unnecessarily broad ruling here.

FACTUAL BACKGROUND

A. Recent Criminal Data Breach Litigation.

Recent years have seen a spate of criminal data breaches in which hackers have stolen and misused personal information pertaining to millions of Americans. Examples include the highly publicized data breaches at Anthem, Yahoo, Target, Neiman Marcus, and Wendy's. In each instance, lawsuits were filed by consumers victimized by identity theft and at risk of future harm and by financial institutions forced to reimburse their customers' fraud losses and reissue compromised credit and debit cards to mitigate future losses. These lawsuits typically assert negligence claims based on the theory it was reasonably foreseeable that criminals would seek to steal customers' personal information and that the data breach would have been prevented by adequate cybersecurity measures.

Three such cases – involving major data breaches at Home Depot, Arby's, and Equifax – have been or are still being litigated in Georgia. *See In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-md-02583-TWT (N.D. Ga. filed 2014); *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-mi-55555-AT (N.D. Ga. filed 2017); *In re Equifax, Inc., Customer Data Security Breach Litig.*, No. 1:17-md-02800-TWT (N.D.G.A. filed 2017). In each case, plaintiffs asserted

claims for negligence based on the defendants' failure to take reasonable steps to prevent a foreseeable risk of harm. Plaintiffs also asserted claims for negligence *per se* based on Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair trade practices such as the failure to maintain adequate data security measures to protect consumer personal information.

Home Depot, Arby's, and Equifax moved to dismiss the negligence claims, arguing Georgia law does not impose a duty to maintain adequate data security. In each case, the argument was rejected. As Judge Thrash explained in *Equifax*:

The Court concludes that, under the facts alleged in the Complaint, Equifax owed a duty of care to safeguard the personal information in its custody. This duty of care arises from the allegations that the Defendants knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures. ... [T]o hold otherwise would create perverse incentives for businesses who profit off of the use of consumers' personal data to turn a blind eye and ignore known security risks.

Equifax, 2019 WL 937735, at *13 (N.D. Ga. Jan. 28, 2019). *See also Arby's*, 2018 WL 2128441, at *5 (N.D. Ga. Mar. 5, 2018) (a legal duty arises from "allegations that a company knew of a foreseeable risk to its data security systems"); *Home Depot*, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) ("To hold that no such duty existed would allow retailers to use outdated security measures ..., leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public").

Equifax also argued that data breach victims do not suffer a legally

cognizable injury. The *Equifax* court expressly rejected that argument, stating:

Each of the Plaintiffs alleges that his or her personally identifiable information was compromised in the Data Breach. Such an injury is cognizable under Georgia law.

Equifax, 2019 WL 937735, at *6. In the court’s view, it is sufficient to establish an injury that a plaintiff’s data “was misused, or likely to be misused,” explaining:

Plaintiffs here have alleged that they have been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. These allegations of actual injury are sufficient to support a claim for relief.

Id. Similar arguments by Arby’s and Home Depot were also rejected. *See Arby’s*, 2018 WL 2128441, at *11 (“monetary losses related to fraudulent charges – unauthorized charges on their accounts, theft of their personal information, and costs associated with detection and prevention of identity theft – are sufficient to survive a motion to dismiss); *Home Depot*, 2016 WL 2897520, at *3 (financial institutions that reissued cards, refunded fraudulent charges, and took action to avoid future harm suffered harm sufficient to confer standing).

B. The Facts And Circumstances Relating To The Equifax Data Breach.

The facts in the Equifax case are typical of other criminal data breach cases, although more egregious, as the Equifax data breach is perhaps the most serious in our nation’s history. From mid-May through the end of July 2017, hackers stole

from Equifax the personal and financial information of nearly 150 million American consumers, including names, addresses, birthdates, Social Security numbers, credit card numbers, driver's license numbers, and tax identification numbers. *Equifax*, 2019 WL 937735, at *1-2. Using this information, "identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit worthiness."² *Id.* at *1.

Plaintiffs allege Equifax had a long-standing, cavalier attitude toward data security and never implemented even basic measures to prevent an obviously foreseeable risk. Indeed, its data security was so deficient experts publicly predicted before the breach occurred that the risk of an imminent breach at Equifax exceeded fifty percent. In the words of Judge Thrash:

Equifax recognized the importance of data security, and the value of the data in its custody to cybercriminals. Equifax observed other major, well-publicized data breaches, including those at Target, Home Depot, Anthem, and its competitor Experian. Equifax held itself out as a leader in confronting such threats, offering "data breach solutions" to businesses. ... Equifax was also the subject of several prior data breaches. From 2010 on, Equifax suffered several different data breach incidents highlighting deficiencies in its cybersecurity

² The relevant facts are described with much greater detail in Judge Thrash's opinion on Equifax's motion to dismiss cited above, the consolidated amended complaint filed by the consumer plaintiffs in the federal case, and reports about the Equifax data breach issued recently by the Majority Staff of the U.S. House Committee on Oversight and Government Reform, and the U.S. Senate Permanent Subcommittee on Investigations. The government reports are cited below. The consumer plaintiffs' complaint ("Complaint") can be viewed at <https://images.law.com/contrib/content/uploads/documents/398/20174/Equifax-consumer-complaint.pdf> (last visited March 12, 2019).

protocol. Given these prior breaches, cybersecurity experts concluded that Equifax was susceptible to a major data breach. Analyses of Equifax's cybersecurity demonstrated that it lacked basic maintenance techniques that are highly relevant to potential data breaches. However, despite these risks, Equifax did little to improve its cybersecurity practices. Equifax's leaders afforded low priority to cybersecurity, spending a small fraction of the company's budget on cybersecurity.

Equifax, 2019 WL 937735, at *2.

The immediate cause of the breach was Equifax's failure to apply a free software patch to fix a known security flaw despite receiving explicit warnings from the software developer and the United States Department of Homeland Security, warnings that were widely circulated within the company. Equifax did nothing for months, allowing the hackers to exploit the flaw. *Id.* Equifax also had software that would have detected the hackers immediately, but the software was not working because Equifax had allowed a security certificate to expire and failed to update the certificate for 19 months.³ Once the certificate was finally updated, the software did its job, leading to the discovery of the criminal activity.

In the aftermath of the breach, Equifax was contrite. Testifying before Congress, the company's CEO, Richard Smith, admitted Equifax had breached its duty to protect consumers' information, stating:

³ See Majority Staff Report of the House Committee on Oversight & Governmental Reform, 115TH Congress, "The Equifax Data Breach," at 3, available at <https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf> (last visited March 12, 2019).

We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility.⁴

Equifax urged consumers to act to protect themselves, establishing a website where consumers could find out if their data was stolen, advising affected consumers to freeze their credit to reduce the risk of future identity fraud (which, to be effective, required consumers to freeze their credit at Experian and TransUnion at a minimum cost of \$10 - \$40 per freeze), and offering consumers credit monitoring through an Equifax subsidiary. Complaint ¶¶ 209, 231, 233, 259-60, 263-64. While many consumers took advantage of this offer, others did not trust Equifax and paid for credit monitoring elsewhere.

The impact of the Equifax breach on consumers has been immense, both in terms of the time, effort, and expense that consumers have incurred protecting themselves and the extent of identity theft and fraud that has resulted. Equifax's current CEO acknowledged the undeniable just last week in testimony to Congress, stating: "I certainly recognize the disruption and impact that the cyberattack caused for U.S. consumers and our customers — and I deeply regret what

⁴ Prepared Testimony of Richard F. Smith before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (October 3, 2017), available at <https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf> (last visited March 12, 2019).

happened.”⁵

Moreover, there is a substantial risk that consumers will continue to be harmed in the future. As one widely-quoted analyst has stated: “On a scale of 1 to 10 in terms of risk to consumers, this is a 10.” Complaint ¶ 4. So long as Social Security numbers are widely used in our financial system, the identities of those victimized by the breach are permanently compromised. Criminals can use the stolen information to commit tax fraud and identity theft; open fraudulent credit cards and loan accounts; obtain a driver’s license in the victim’s name but with another’s picture; get a job in the victim’s name; or submit false insurance claims.

The serious risks to the entire economy have drawn scrutiny from Congressional investigators and led to recommendations that the use of Social Security numbers in financial transactions be reduced. In December, 2018, for example, the House Oversight Committee issued a scathing report concluding that (1) as a credit reporting agency, Equifax had a “heightened responsibility to protect consumer data by providing best-in-class data security”; (2) Equifax “failed to implement an adequate security program to protect this sensitive data”; and (3) had “the company taken action to address its observable security issues prior to this

⁵ Written Testimony of Mark Begor, Chief Executive Officer of Equifax Inc., before the U.S. Senate Committee on Homeland Security & Government Affairs Permanent Subcommittee on Investigations (March 7, 2019), available at <https://www.hsgac.senate.gov/imo/media/doc/Begor%20Testimony.pdf> (last visited March 12, 2019).

cyberattack, the data breach could have been prevented.”⁶ And, just last week, the Permanent Subcommittee on Investigations of the U.S. Senate Committee on Homeland Security and Governmental Affairs issued a report entitled “How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach,” which details the extensive failures at Equifax that caused the breach.⁷

ARGUMENT

Amici respectfully suggest that this case is not an appropriate place for this Court to weigh in on the issues of legal duty and injury that arise in criminal data breach litigation. That is because this case does not involve allegations of inadequate data security, the foreseeability of a criminal intrusion, actual identity theft and a substantial risk of future harm. The legal arguments that flow from such allegations are therefore not developed in the record, and it is unnecessary to decide issues of duty and injury in criminal data breach cases to resolve this appeal. Moreover, Amici suggest that this Court be cautious about drawing broad conclusions that could affect the rights of litigants in criminal data breach cases, particularly in light of the developing national consensus in such cases recognizing an enforceable legal duty and finding legally cognizable injuries.

⁶ *See supra* note 3, at 2-4.

⁷ Available at: <https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf> (last visited March 12, 2019).

A. The Facts And Circumstances In This Case Are Starkly Different Than In Criminal Data Breach Cases Such As *Equifax*.

Extensive allegations of foreseeable risk and harm clearly distinguish a typical criminal data breach case from the case now before the Court. Here, a Department of Labor employee accidentally attached confidential information to an email sent to 1,000 recipients. There is no allegation of the foreseeable criminal activity and systemic cybersecurity lapses described above. Further, there are no credible allegations that the email's recipients have misused or will misuse the information that was inadvertently disclosed.

The factual differences between this case and *Equifax* are even more substantial. For example, Equifax is not a government agency, but a company whose core business involves collecting and profiting from the sale of massive amounts of consumer data and knew of the critical need to safeguard that data to protect the American economy. The head of the Department of Labor, unlike Equifax's CEO, never admitted his agency had an "enormous responsibility" to protect the data involved. The scope of the information disclosed is not comparable (e.g. disclosure of limited data pertaining to a few thousand people versus disclosure of the most sensitive consumer information pertaining to more than half of the nation's adult population); the risk of future harm is of a different magnitude (e.g. in this case there is no good reason to believe anyone will misuse the information while the risk from the Equifax breach is so substantial that

Congress is discussing eliminating the use of Social Security numbers); and, unlike the Department, Equifax acknowledged the substantial future risk by urging consumers to take protective action, such as obtaining credit monitoring services.

In addition to the underlying factual distinctions between this case and criminal data breach cases, the legal obligations that apply to private parties are quite different than those that apply to the Department of Labor. For instance, the typical defendant in a criminal data breach case has a legal duty under Section 5 of the FTC Act to maintain adequate data security measures to protect consumers, *see, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015); the FTC has adopted regulations pursuant to the Gramm-Leach-Bliley Act requiring financial institutions to protect consumer information, *see Equifax*, 2019 WL 937735, at *12; companies that accept consumers' credit cards are bound by contract with the card associations such as VISA and MasterCard to comply with industry-wide data security standards, *see generally, e.g., Pennsylvania State Employees Credit Union v. Fifth Third Bank*, 2006 WL 1724574, at *6 (M.D. Pa. Jun. 16, 2006); and the Fair Credit Reporting Act strictly limits the ability of a credit reporting agency such as Equifax to disclose consumer information. *Equifax*, 2019 WL 937735, at *12.

These factual and legal differences are critical for purposes of assessing the duty element of a negligence claim in a criminal data breach case. The

foreseeability and extent of potential harm, in many ways, is the *sine qua non* of the duty analysis. *See, e.g., Underwood v. Select Tire, Inc.*, 296 Ga. App. 805, 809 (2009) (“Neither duty nor negligence exists in a vacuum—they are entirely dependent upon circumstances involving others or their property.”) (internal quotation omitted); *Amos v. City of Butler*, 242 Ga. App. 505, 506 (2000) (“Negligence is predicated on what should be anticipated, rather than on what happened, because one is not bound to anticipate or foresee and provide against what is unlikely, remote, slightly probable, or slightly possible. ... [T]he legal duty to exercise ordinary care arises from the foreseeable unreasonable risk of harm from such conduct.”). Furthermore, whether a common law duty exists can turn on obligations imposed by federal law. *See Pulte Home Corp. v. Simerly*, 322 Ga. App. 699, 705-06 (2006) (“violations of federal statutes and regulations support [a] claim of breach of legal duty in both traditional negligence and negligence per se actions”).

In similar fashion, the factual differences are critical for assessing the legal sufficiency of the alleged injuries. In this case, not only is there no credible allegation that the information disclosed by the Department has been misused, there is no plausible allegation of a substantial or imminent risk it will ever be misused. In contrast, in *Equifax* and other like cases consumers suffered fraud and identity theft after the breach and because the breach was carried out by criminals

there are compelling reasons to conclude that such fraud and identity theft will continue to occur. To paraphrase the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015): Why would criminal hackers break into a company’s databases and steal consumers’ private information unless they intended to use it for nefarious purposes? Moreover, Equifax itself has acknowledged the substantial risk of future harm by advising those affected to take protective action and offering them free credit freezes and credit monitoring. *See, e.g., Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 388 (6th Cir. 2016) (by offering credit monitoring services to consumers after a breach the defendant recognized the severity of the risk of future harm).

These extensive factual and legal differences – and their impact on the issues of duty and injury – led the courts in *Arby’s* and *Equifax* to reject arguments that the Court of Appeals’ decisions in this case required dismissal of plaintiffs’ negligence claims. *Arby’s* distinguished this case because the facts here are “starkly different.” 2018 WL 2128441 at *6. *Equifax* came to the same conclusion, emphasizing “a critical distinction” in the duty analysis that arises “from allegations that the defendant failed to implement reasonable security measures in the face of a known security risk.” 2019 WL 937735, at *13. In fact, Judge Thrash specifically declined Equifax’s request that he delay a decision until after this Court decides this appeal because of the dissimilarities between the

allegations in *Equifax* and this case, explaining:

[I]t seems very unlikely to me that the Georgia Supreme Court will adopt a rule of law that tells hundreds of millions of consumers in the United States that a national credit reporting agency headquartered in Georgia has no obligation to protect their confidential personal identifying data. Unlike the Georgia Department of Labor, Equifax and the other credit reporting agencies are heavily regulated by federal law [referring to the Fair Credit Reporting Act, Section 5 of the FTC Act, and regulations adopted under the Gramm-Leach-Bliley Act].

Id. at *12.⁸

Even the Department of Labor has taken the position that *Arby's* and *Home Depot* – and by extension, the decision in *Equifax* issued after the Department's brief was filed – are “too factually distinguishable to apply here.” See January 15, 2019 Brief of Appellee, No. S18G1317, at 15. According to the Department, those cases concern “the factually distinguishable scenario of whether retail merchants should have foreseen the risk of third party ‘hackers’ intercepting their customers’ personal information” and, unlike in Mr. McConnell's case, “both *Home Depot* and *Arby's* involved claims of actual theft of consumers' financial data by third party hackers, including unauthorized debit and credit card charges and disabled accounts.” *Id.*

In short, because *Equifax*, *Arby's*, *Home Depot*, and similar criminal data breach cases turn on legal analysis arising out of materially different facts and

⁸ In *Equifax*, Judge Thrash has found that Georgia common law governs the claims of all the consumer plaintiffs, regardless of the state in which an individual plaintiff was injured. *Equifax*, 2019 WL 937735, at *3.

dramatically different circumstances bearing on the issues of duty and injury, this Court should be cautious about venturing into those issues in this case, particularly since it is unnecessary to resolve this appeal.⁹

B. The Court Should Not Address The Merits Of A Negligence Claim In A Criminal Data Breach Case Based On The Record In This Case.

Another reason why this Court should avoid analyzing the issues of duty and injury that govern in criminal data breach cases is that neither the record below nor the legal arguments of the parties in their briefing here are sufficiently developed to allow a meaningful analysis, consistent with the customary appellate process. *See generally Chrysler Grp., LLC v. Walden*, 303 Ga. 358, 372 (2018) (“[T]he cardinal principle of judicial restraint” is “if it is not necessary to decide more, it is necessary not to decide more”).

It is hardly surprising that the record and legal arguments related to criminal data breaches are undeveloped here. The Department of Labor did not address criminal data breach litigation except to distinguish *Arby's* and *Home Depot*

⁹ In its first decision, the Court of Appeals itself distinguished *Home Depot* on the ground that there are no allegations in this case that “the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years.” 337 Ga. App. 457, 459 n.4 (2016). In its latest decision, the Court of Appeals came to the same conclusion regarding the merits of the plaintiffs’ negligence claim, but did not discuss or attempt to distinguish *Home Depot*. The Court of Appeals’ silence suggests its tacit recognition that the issue of duty in criminal data breach cases is subject to an entirely different analysis. *See Equifax*, 2019 WL 937735, at *13.

because, as noted above, it believes such litigation is too unlike this case to be instructive. Mr. McConnell only touches on some of the particularized legal arguments that apply in a criminal data breach case. And, neither the trial court nor the Court of Appeals considered how the issues of duty or injury involved here would impact a criminal data breach case, except for a footnote in the Court of Appeals' first opinion distinguishing this case from *Home Depot*.

The Court of Appeals' discussion of the duty issue in its most recent opinion is illustrative. In concluding that the Department of Labor owes no legal duty to protect personal information, the Court of Appeals focused entirely on two Georgia statutes that Mr. McConnell argued create the duty. The Court of Appeals disagreed with Mr. McConnell, finding that Georgia's data breach notification statute, O.C.G.A. § 10-1-910, does not impose any standards regarding data security and the Georgia Fair Business Act, O.C.G.A. § 10-1-393.8, only prohibits the intentional, not inadvertent, disclosure of a Social Security number. *McConnell*, 345 Ga. App 669, 675-79 (2018). The legal duty to employ adequate cybersecurity measures recognized in criminal data cases does not arise from those very specific statutes, but from much broader principles such as the common law duty not to subject others to an unreasonable risk of harm, the existence of applicable industry standards, and the obligations imposed by federal statutes and regulations. The Court of Appeals did not discuss any of these matters.

Likewise, the Court of Appeals’ analysis of the legal sufficiency of the alleged injuries suffered by Mr. McConnell is not particularly helpful in evaluating whether victims of a criminal data breach have suffered legally cognizable injury. The Court of Appeals did not analyze the sufficiency of Mr. McConnell’s injury to address the merits of his negligence claim, but to determine whether his alleged injuries constituted a “loss” within the meaning of the Georgia Tort Claims Act. While the Department argued that the time, effort and money Mr. McConnell spent monitoring his credit and the risk of future injury he allegedly faces are not actual damages, the Court of Appeals did not have to decide whether the Department was correct because Mr. McConnell had another alleged injury – financial loss from a drop in his credit score – that was sufficient to establish subject matter jurisdiction under the Tort Claims Act. *McConnell*, 345 Ga. App. at 673-74.

C. This Court Should Be Cautious About Potentially Restricting Claims Of Criminal Data Breach Victims Widely Allowed In Other Courts.

Equifax, *Arby’s*, and *Home Depot* are not the only cases that have refused to dismiss negligence claims brought by victims of criminal data breaches. While there are a few outliers, the emerging judicial consensus is that companies have a legal duty to use reasonable efforts to protect confidential consumer information

from foreseeable harm such as the risk of a criminal data breach.¹⁰ In addition, there is a substantial body of other case law across the country establishing that criminal data breach victims whose personal information is stolen have suffered a legally cognizable injury and may recover for their time, effort and money spent redressing identity theft and fraud that has occurred¹¹ and mitigating a substantial

¹⁰ See, e.g., *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) (“It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information”); see also, e.g., *Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 423-27 (5th Cir. 2013); *S. Indep. Bank v. Fred’s Inc.*, 2016 WL 11164794, at *3-4 (M.D. Ala. Sept. 23, 2016); *In re Experian Data Breach Litig.*, 2016 WL 7973595, at *3, *5, *7, *8 (C.D. Cal. Dec. 29, 2016); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015); *Hapka v. CareCentrix, Inc.*, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016); *Savidge v. Pharm-Save, Inc.*, 2017 WL 5986972, at *3 (W.D. Ky. Dec. 1, 2017); *Banknorth, N.A. v. BJ’s Wholesale Club, Inc.*, 394 F. Supp. 2d 283, 286-87 (D. Me. 2005); *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1308-10 (D. Minn. 2014); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 747-48 (S.D.N.Y. 2017); *Jones v. Commerce Bancorp, Inc.*, 2006 WL 1409492, at *2 (S.D.N.Y. May 23, 2006).

¹¹ See, e.g., *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323-24 (11th Cir. 2012); *Arby’s*, 2018 WL 2128441, at *11 n.12; *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 165-67 (1st Cir. 2011); *Hutton v. Nat’l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622, 623 n.9 (4th Cir. 2018); *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018); *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016); *Remijas*, 794 F.3d at 692-94; *Smith v. Triad of Alabama, LLC*, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *14-16 (N.D. Cal. Aug. 30, 2017); *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *14-15 (N.D. Cal. May 27, 2016); *Experian*, 2016 WL 7973595, at *5; *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 345 (W.D.N.Y. 2018).

risk of future harm, such as by purchasing credit monitoring services.¹²

Amici bring this case law to the Court's attention to show that victims of a criminal data breach are routinely permitted to pursue negligence claims against companies that do not use reasonable cybersecurity measures to protect consumers' confidential information. To avoid the risk of Georgia being seen as out of step with the way in which courts around the country approach criminal data breach litigation, Amici suggest that the Court not use broad language that is unnecessary to the result and could be applied to restrict the claims of plaintiffs in criminal data breach cases.

CONCLUSION

For the reasons set forth above, Amici request the Court expressly limit its decision to the specific facts and legal claims at issue on appeal. Whether the Department of Labor owed any legal duty or Mr. McConnell suffered legally cognizable injuries are questions that can – and Amici respectfully suggest should – be answered without potentially adversely impacting what happens in *Equifax* and similar criminal data breach cases.

¹² See, e.g., *Anderson*, 659 F.3d at 165-66; *Hutton*, 892 F.3d at 622; *Remijas*, 794 F.3d at 692-94; *Yahoo!*, 2017 WL 3727318, at *16; *Anthem*, 2016 WL 3029783, at *16; see also *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013).

Respectfully submitted,

Amy E. Keller
**DiCELLO LEVITT
GUTZLER LLC**
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dicellolevitt.com

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
**DOFFERMYRE SHIELDS
CANFIELD & KNOWLES, LLC**
1355 Peachtree Street, N.E., Suite 1725
Atlanta, Georgia 30309
Tel. 404.881.8900
kcanfield@dsckd.com

Norman E. Siegel
Barrett J. Vahle
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel. 816.714.7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com

***Consumer Plaintiffs' Co-Lead Counsel
Equifax Data Breach Multi-District Litigation***

/s/ Roy E. Barnes
Roy E. Barnes
J. Cameron Tribble
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Tel. 770.227.6375
roy@barneslawgroup.com
ctribble@barneslawgroup.com

/s/ David J. Worley
David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350
Tel. 404.205.8400
david@ewlawllc.com

***Consumer Plaintiffs' Co-Liaison Counsel
Equifax Data Breach Multi-District Litigation***

Andrew N. Friedman
**COHEN MILSTEIN SELLERS &
TOLL PLLC**
1100 New York Avenue, NW
Suite 500
Washington, D.C. 20005
Tel. 202.408.4600
afriedman@cohenmilstein.com

Eric H. Gibbs
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612
Tel. 510.350.9700
ehg@classlawgroup.com

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Ariana J. Tadler
**MILBERG TADLER PHILLIPS
GROSSMAN LLP**
One Penn Plaza
19th Floor
New York, New York 10119
Tel. 212.594.5300
atadler@milberg.com

John A. Yanchunis
**MORGAN & MORGAN COMPLEX
LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. 813.223.5505
jyanchunis@forthepeople.com

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224
Tel. 410.539.6500
hassan.murphy@murphyfalcon.com

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
Tel. 770.578.1314
jasondoss@dossfirm.com

*Consumer Plaintiffs' Steering Committee
Equifax Data Breach Multi-District Litigation*

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, Georgia 30303
Tel. 404.584.9777
rodney@gspclaw.com

*Consumer Plaintiffs' State Court Coordinating Counsel
Equifax Data Breach Multi-District Litigation*

CERTIFICATE OF SERVICE

I hereby certify that I have, this day, filed the foregoing **AMICUS CURIAE BRIEF OF THE CONSUMER PLAINTIFFS IN THE EQUIFAX DATA BREACH MULTI-DISTRICT LITIGATION** upon all counsel of record by filing a true and correct copy thereof with the Clerk of Court using the SCED online system and served the following counsel by depositing copies of the same in the United States Postal Service with adequate First-Class Mail postage thereon and addressed as follows:

Christopher M. Carr, *Attorney General*
Kathleen M. Pacious, *Deputy Attorney General*
Loretta L. Pinkston-Pope, *Senior Assistant Attorney General*
Ellen Cusimano, *Assistant Attorney General*
OFFICE OF THE ATTORNEY GENERAL
40 Capitol Square, SW
Atlanta, Georgia 30334
Counsel for Georgia Department of Labor

Scott A. Schweber, Esq.
SCHWEBER GREEN LAW GROUP
2002 Summit Boulevard, Suite 300
Atlanta, Georgia 30319
Counsel for Thomas McConnell, et al.

Jefferson M. Allen, Esq.
COHEN, COOPER, ESTEP & ALLEN, LLC
3330 Cumberland Boulevard, Suite 600
Atlanta, GA 30339
Counsel for Thomas McConnell, et al.

This 14th day of March, 2019.

/s/ Roy E. Barnes

Roy E. Barnes

BARNES LAW GROUP, LLC

31 Atlanta Street

Marietta, Georgia 30060

Tel. 770.227.6375

roy@barneslawgroup.com

Attorney for *Amici Curiae*

Consumer Plaintiffs in Equifax Data

Breach Multi-District Litigation

EXHIBIT B

March 30, 2019 Term Sheet

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

**Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives**

**CONFIDENTIAL SETTLEMENT TERM SHEET
RULE 408 PROTECTED COMMUNICATION**

Re: *In re: Equifax, Inc. Customer Data Security Breach Litigation,
MDL No. 2800 (Consumer Cases)*

- I. Settlement Class:** Subject to confirmatory discovery, the Settlement Class for Individuals shall be defined as: “The approximately 148 million U.S. consumers identified by Equifax whose personal information was compromised as a result of the cyberattack and data breach announced by Equifax on September 7, 2017.”
- II. Settlement Consideration:**
- A. Settlement Fund:** Within 10 days of the effective date of the settlement, Equifax will fund a non-reversionary Settlement Fund to be administered by the Settlement Administrator in the amount of \$310 million.
- 1. Use of Settlement Fund:** Except as specifically provided below, the Settlement Fund will be used to fund the settlement provisions listed in sections **II.B, II.D.2, II.D.3, IV, and V**. Equifax will separately pay all other costs of the Settlement. To the extent the aggregate amounts required to fund the settlement provisions listed in sections **II.B** and **II.D.3** exceed the amount of the Settlement Fund remaining after distributions are made to fund the settlement provisions listed in sections **II.D.2, IV** and **V**, the cash payments provided in these provisions shall be reduced on a *pro rata* basis in a manner to be negotiated.
 - 2. Use of Remaining Settlement Funds:** Any remaining funds in the Settlement Fund after the payments described in sections **II.B, II.D.2, II.D.3, IV, and V** and after the conclusion of the Extended Claims Deadline will be used as follows:
 - a. First, the percentage caps in sections **II.B.2.f** and **II.D.3** will be lifted (if applicable) and payments increased *pro rata* to Class members with valid claims up to the full amount of the approved claim submitted under those sections.
 - b. Second, if the payment described in section **II.A.2.a** does not exhaust the Settlement Fund, up to 36 months of additional credit monitoring services (purchased in full-month increments) will be provided to those who have filed a valid claim for such services under section **II.D.2** and up to five years of additional fraud restoration services (purchased in full-month increments) will be provided to the class.
 - c. Third, if the payments described in sections **II.A.2.a** and **II.A.2.b** do not exhaust the Settlement Fund (there being insufficient funds to purchase the

next full month increment of credit monitoring and restoration services as provided in **II.A.2.b**), then any remaining funds shall be used to provide additional benefits to the class to be agreed by the parties.

B. Reimbursement for Out-of-Pocket Losses.

1. The Settlement Administrator will use the Settlement Fund to compensate those Class members who submit valid claims for Out-of-Pocket Losses fairly traceable to the data breach announced by Equifax on September 7, 2017 (the “Data Breach”). Individual claimants will be subject to an aggregate claims cap of \$20,000 paid directly from the Settlement Fund regardless of the number of claims submitted by the claimant during the Initial Claims Period and Extended Claims Period. This provision does not prevent Class members from submitting claims under applicable insurance policies.
2. “Out-of-Pocket Losses” are verifiable unreimbursed costs or expenditures that a Class member actually incurred and that are fairly and reasonably traceable to the Data Breach. Out-of-Pocket Losses may include, without limitation, the following:
 - a. unreimbursed costs, expenses, losses or charges incurred a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of Class members’ personal information;
 - b. costs incurred on or after September 7, 2017, associated with freezing or unfreezing credit report with any credit reporting agency;
 - c. other miscellaneous expenses incurred related to any Out-Of-Pocket Loss such as notary, fax, postage, copying, mileage, and long-distance telephone charges;
 - d. credit monitoring costs that were incurred on or after September 7, 2017, through the date of the Class member’s claim submission;
 - e. up to 25% reimbursement for costs incurred by a class member who purchased Equifax credit or identity monitoring subscription products in the 12 months preceding September 7, 2017 and who had such subscriptions in place at any point in time between May 13, 2017 to September 7, 2017;
 - f. subject to the provisions of section **III.B.2**, up to 20 total hours for time spent taking Preventative Measures and time spent remedying fraud, identity theft, or other misuse of a Class member’s personal information that is fairly traceable to the Data Breach at \$25 per hour. Up to 10% of the Settlement Fund will be used to compensate Class members for time under this section.

If the settlement payments for time exceed this amount, then payments for time shall be distributed *pro rata* to those making valid claims for time.

C. Credit freezes and unfreezes.

All Class members will be eligible to receive free access to Equifax's credit freezes and credit unfreezes for Equifax credit files, enforceable under the Settlement for 10 years without filing a claim.

D. Credit monitoring and fraud resolution services.

1. Separate from and in addition to the Settlement Fund, Equifax has provided Class members who enrolled in Trusted ID monitoring provided by Equifax following the breach with an additional one year of credit monitoring services known as IDNotify to allow for continuity of these services while the parties finalize the settlement.
2. All Class members will be eligible to claim and enroll in at least 3 years of additional credit monitoring services provided by a party with which Equifax is not affiliated and in which Equifax has no financial interest. Equifax will provide its data necessary to carry out these services to the third party monitor free of charge. The provider for credit monitoring services shall include the services in Exhibit A and consistent with the standards set forth in Exhibit A. The provider for credit monitoring services will also provide to all Class members (regardless of whether the Class member makes any claim under the Settlement) access to a U.S. based call center providing fraud resolution services relating to identity theft, fraud and identity restoration throughout the same period.
3. Class members who already have some form of credit monitoring or protection and do not claim the credit monitoring services available under section **II.D.1** may file a claim for alternative compensation of \$100. The Class member must identify the monitoring service and certify that he or she has some form of credit monitoring or protection as of the date the Class member submits the claim and will have such credit monitoring in place for a minimum of 6 months from the claim date. Class members who elect to receive alternative compensation under this provision are not eligible to enroll in credit monitoring services offered under section **II.D.2** or to seek reimbursement for the same products submitted for reimbursement pursuant to section **II.B.2.d**. Up to 10% of the Settlement Fund will be used to provide alternative compensation to Class members under this provision. If the settlement payments for alternative compensation under this provision exceed the cap set forth in the preceding sentence, then payments for such alternative compensation shall be distributed *pro rata* to those making valid claims for alternative compensation.
4. Claims for credit monitoring and alternative compensation can be made only within the Initial Claims Period.

5. To the extent the number of enrollees in the third party credit monitoring exceeds 7 million, Equifax will pay the costs of providing 3 years of credit monitoring for all enrollees in excess of 7 million on the terms described in Section **II.D.2** separate from and in addition to the Settlement Fund.

E. Business practice commitments.

1. Equifax will adopt, pay for, implement, and/or maintain the minimum business practice commitments related to information security to safeguard Class members' Personal Information as defined and as set forth in Exhibit B.
2. Equifax's business practice commitments will be submitted in a form that permits independent supervision and judicial enforcement of Equifax's commitments.
3. From the effective date of the settlement and for a period of five years thereafter, neither Equifax nor any of its affiliated companies will use or seek to enforce any arbitration provision or class action waiver in any Equifax product or service offered in response to the Data Breach or otherwise provided by Equifax under this settlement against consumers for claims related to or arising from the Data Breach. This provision cannot be superseded or modified by any agreement pertaining to any other Equifax product or service or any product or service offered by one of Equifax's affiliates, parents, successors, agents, subsidiaries, or assigns.
4. Equifax will implement a program to provide prompt notice of any future breaches of consumer information consistent with the requirements of all Federal and State regulations.

III. Claims Process:

A. Claims for Reimbursement for Out-of-Pocket Losses under II.B.

1. The Settlement Administrator shall evaluate claims and make a determination as to whether claimed Out-of-Pocket Losses are valid and fairly traceable to the Data Breach. The Parties will negotiate a reasonably practical procedure for the Settlement Administrator to determine whether the Settlement Class member's claimed Out-of-Pocket Losses are compensable under the terms of the Settlement. The parties agree that the goal of the claims procedure is to facilitate payment of properly submitted claims. The Parties shall negotiate a notice and appeal process for review of the Claim Administrator's claims determinations.

2. Out-of-Pocket Losses associated with freezing or unfreezing credit reports (**II.B.2.b**) and purchasing credit monitoring services (**II.B.2.d**) (“Preventative Measures”), shall be deemed fairly traceable to the Data Breach if (i) they were incurred on or after September 7, 2017, through the date of the Class member’s claim submission, and (ii) the claimant certifies that they incurred such Out-of-Pocket Losses as a result of the Data Breach and not as a result of any other compromise of the Class member’s information.

B. Documentation needed to submit claims for Out-of-Pocket Losses:

1. Class members with Out-of-Pocket Losses must submit Reasonable Documentation supporting their claims. As used herein, “Reasonable Documentation” means documentation supporting a claim prepared by a third party. Non-exhaustive examples of Reasonable Documentation include credit card statements, bank statements, invoices, telephone records, and receipts. Except as expressly provided herein, personal certifications, declarations, or affidavits from the claimant do not constitute Reasonable Documentation but may be included to provide clarification, context or support for other submitted Reasonable Documentation.
2. Class members who spent time remedying fraud, identity theft, or other alleged misuse of the Class member’s personal information fairly traceable to the Data Breach, or who spent time on Preventative Measures fairly traceable to the Data Breach can receive reimbursement for such time expenditures subject to the following provisions.
 - a. Documented Time. Class Members with (i) Reasonable Documentation of fraud, identity theft, or other alleged misuse of the Class member’s personal information fairly traceable to the Data Breach and (ii) time spent remedying these issues, or time spent taking Preventative Measures, may submit a claim for up to 20 hours of such time to be compensated at \$25 per hour.
 - b. Self-Certified Time. Class Members who attest to fraud, identity theft, or other alleged misuse of the Class member’s personal information fairly traceable to the Data Breach, or taking Preventative Measures, but who cannot provide Reasonable Documentation of such issues may self-certify the amount of time they spent remedying the foregoing and file a claim for up to 10 hours at \$25 per hour.

C. Claims Periods. There will be two claims periods: the Initial Claims Period and the Extended Claims Period.

1. The **Initial Claims Period** will run for six months after the notice deadline.
2. The **Extended Claims Period** will run for up to three years after the conclusion of the Initial Claims Period. During the Extended Claims Period, Class members


can seek reimbursement for Out-of-Pocket Losses (excluding losses associated with Preventative Measures) incurred during the Extended Claims Period if the following prerequisites are met: (i) the Class member claimed credit monitoring services offered under the settlement, or submits Reasonable Documentation showing that he or she had some form of credit monitoring or protection at the time of the loss; and (ii) the Class member provides a certification that he or she has not obtained reimbursement for the claimed expense through other means.

- IV. Attorneys' Fees and Expenses.** Plaintiffs, through Plaintiffs' Lead Consumer Counsel, will seek 25% of the Settlement Fund to pay reasonable attorneys' fees performed by Lead Consumer Plaintiffs' Counsel or other counsel working at their direction in connection with this litigation. In addition to fees, Plaintiffs will also request reimbursement of reasonable costs and expenses in connection with the litigation up to \$3 million. Plaintiffs' Lead Counsel will make such applications as provided under the Federal Rules and Equifax agrees not to take a position on such applications.
- V. Administration and Class Notice Costs.** The Administration and Class Notice Costs will be paid from the Settlement Fund, provided however that if the amount of any such Class Notice Costs exceeds \$20 million either party may terminate this agreement.
- VI. Releases.** Mutual releases, to the fullest extent permitted by law, will be negotiated and included in the final Settlement Agreement.
- VII. Status of Agreement.** This is a binding Term Sheet, although the parties hereto intend to further document the agreement in a comprehensive written agreement containing additional details regarding the notice program, administration, and implementation of the Settlement as well as additional provisions of the type typically used in class action settlements ("Settlement Agreement"). Upon execution of this Term Sheet, the parties shall mutually inform the Court that the parties have reached an agreement to settle this litigation and that the Settlement Agreement will be presented to the Court for preliminary approval 90 days after the date of this Term Sheet. The parties agree to work together in good faith in drafting and executing the Settlement Agreement as soon as practicable but not more than 60 days after the date of this Term Sheet, provided, however, that this time period will be extended in response to a Regulator request for a reasonable extension of time. Prior to submission of preliminary approval, Plaintiffs agree to keep the settlement and its terms confidential, except that they may jointly with Equifax discuss the Term Sheet with Regulators, or for such disclosure as the Court may require. Plaintiffs agree that Equifax may disclose the terms of the settlement, including the executed Term Sheet, to the Federal Trade Commission, the Consumer Financial Protection Bureau, state Attorneys General and other government regulators (collectively, "Regulators") prior to submission of preliminary approval. The parties agree that, to the extent that the Regulators propose changes to the class benefits or the Term Sheet, Plaintiffs will discuss and consider in good faith such changes, and if the parties agree, the Term Sheet/Settlement Agreement will be amended accordingly. The parties agree to bring any disputes that arise in the process of drafting the Settlement Agreement to mediator Layn Phillips. To the extent the parties cannot resolve any

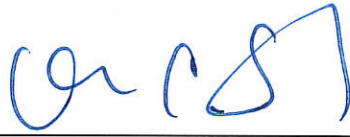
dispute through mediation, the parties shall submit competing proposals to Layn Phillips for a final determination, which shall be binding on the parties for purposes of the Settlement Agreement.

VIII. Service Awards. Plaintiffs will seek service awards, to be approved by the Court, in an amount to be negotiated by the parties. Any such service awards will be paid from the Settlement Fund.

AGREED TO AND ACCEPTED:


By: JOHN J. KEWEY III
Equifax Inc.

Date: March 30, 2019


By: NORMAN F. SIEGEL
For Plaintiffs

Date: MARCH 30, 2019

TERM SHEET EXHIBIT B EQUIFAX BUSINESS PRACTICE CHANGES

Unless otherwise specified below, the following security measures or their equivalents will be deployed and maintained by Equifax for at least 5 years from the date the District Court grants final approval of the Settlement Agreement unless otherwise specified below:

- 1** **Scope:** This Agreement shall apply to all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of accessing, using or sharing software, data, and hardware resources; (2) are owned, operated, and/or controlled by Equifax; and (3) collect, process, store, have access, or grant access to Personal Information of consumers who reside in the United States, but excluding networking equipment, databases or data stores, applications, servers, or endpoints outside of the U.S. where access to Personal Information is restricted using a risk-based control (“Equifax Network”).
 - a. “Personal Information” shall have the same meaning as set forth in the data privacy laws in the states in which Class Members reside, unless preempted by federal law.
 - b. The “NIST Standard” refers to the most recent applicable NIST guidance, beginning with NIST 800-53r4, as the primary set of standards, definitions, and controls. Where this Agreement requires Equifax to test cyber resilience, Equifax will use an industry- recognized cybersecurity framework (for example, NIST CSF framework). Where this Agreement refers to “NIST or another comparable standard,” Equifax either will use the NIST standard indicated above or another industry-recognized cybersecurity standard that satisfies Regulator Requirements.
 - c. “Regulator” means the Federal Trade Commission (“FTC”), the Consumer Financial Protection Bureau (“CFPB”), or the multi-state group of state Attorneys General investigating the 2017 Data Breach. If no Regulator is willing or able to make a determination under this Agreement, then one of the attorneys designated as Co-Lead Counsel for the Consumer Plaintiffs in this multi-district litigation, or their law firms, and Equifax’s CISO or their designee shall, in good faith, reach a determination.

- 2** **Information Security Program:** Within ninety (90) days of final approval, Equifax shall implement, and thereafter regularly maintain, review, and revise a comprehensive Information Security Program that is reasonably designed to protect the confidentiality, integrity, and availability of the Personal Information that Equifax collects, processes, or stores on the Equifax Network.

- 3** **Managing Critical Assets:** Equifax shall identify and document a comprehensive IT asset inventory, using an automated tool(s) where practicable, that, consistent with NIST or another comparable standard, will inventory and classify, and issue reports on, all assets that comprise the Equifax Network, including but not limited to software, applications, network components, databases, data stores, tools, technology, and systems. The asset inventory required under this paragraph shall be regularly updated and, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset’s location within the Equifax Network; and (e) the asset’s criticality rating. Equifax shall maintain, regularly review and revise as necessary, and comply with

- a Governance Process¹ establishing that hardware and software within the Equifax Network be rated based on criticality, factoring in whether such assets are used to collect, process, or store Personal Information. Equifax shall comply with this provision by June 30, 2020.
- 4 **Data Classification:** Equifax shall maintain and regularly review and revise as necessary a data classification and handling standard.
 - 5 **Security Information and Event Management:** Consistent with NIST or another comparable standard, Equifax shall implement a comprehensive, continuous, risk-based SIEM solution (or equivalent). Equifax shall continuously monitor, and shall test on at least a monthly basis, any tool used pursuant to this paragraph, to properly configure, regularly update, and maintain the tool, to ensure that the Equifax Network is adequately monitored.
 - 6 **Logging and Monitoring:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing: (1) risk-based monitoring and logging of security events, operational activities, and transactions on the Equifax Network, (2) the reporting of anomalous activity through the use of appropriate platforms, and (3) requiring tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance. The Governance Process shall include the classification of security events based on severity and appropriate remediation timelines based on classification.
 - 7 **Vulnerability Scanning:** Equifax shall implement and maintain a risk-based vulnerability scanning program reasonably designed to identify and assess vulnerabilities within the Equifax Network.
 - 8 **Penetration Testing:** Equifax shall implement and maintain a risk-based penetration-testing program reasonably designed to identify and assess security vulnerabilities within the Equifax Network.
 - 9 **Vulnerability Planning:** Equifax shall rate and rank the criticality of all vulnerabilities within the Equifax Network. For each vulnerability that is ranked most critical, Equifax shall commence remediation planning within twenty-four (24) hours after the vulnerability has been rated as critical and shall apply the remediation within one (1) week after the vulnerability has received a critical rating. If the remediation cannot be applied within one (1) week after the vulnerability has received a critical rating, Equifax shall identify or implement compensating controls designed to protect Personal Information as soon as practicable but no later than one (1) week after the vulnerability received a critical rating.
 - 10 **Patch Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process to maintain, keep updated, and support the software on the Equifax Network. Equifax shall maintain reasonable controls to address the potential impact that security updates and patches may have on the Equifax Network

¹ “Governance Process” shall mean any written policy, standard, procedure or process (or any combination thereof) designed to achieve a control objective with respect to the Equifax Network.

and shall maintain a tool that includes an automated Common Vulnerabilities and Exposures (CVE) feed with regular updates regarding known CVEs.

- 11 Threat Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing a threat management program designed to appropriately monitor the Equifax Network for threats and assess whether monitoring tools are appropriately configured, tested, and updated.
- 12 Access Control and Account Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to appropriately manage Equifax Network accounts. This Governance Process shall include, at a minimum, (1) implementing appropriate password, multi-factor, or equivalent authentication protocols; (2) implementing and maintaining appropriate policies for the secure storage of Equifax Network account passwords, including policies based on industry best practices; and (3) limiting access to Personal Information by persons accessing the Equifax Network on a least-privileged basis.
- 13 File Integrity Monitoring:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to provide prompt notification of unauthorized modifications to the Equifax Network.
- 14 Legacy Systems:** Equifax shall develop and implement a risk-based plan to remediate current legacy systems on a schedule that provides for remediation within five years following final approval of this Agreement and which includes applying compensating controls until the systems are remediated. Equifax shall also maintain a Governance Process for active lifecycle management for replacing and deprecating legacy systems when they reach end of life.
- 15 Encryption:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process requiring Equifax either to encrypt Personal Information or otherwise implement adequate compensating controls.
- 16 Data Retention:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing a retention schedule for Personal Information on the Equifax Network and a process for deletion or destruction of Personal Information when such information is no longer necessary for a business purpose, except where such information is otherwise required to be maintained by law.
- 17 TrustedID Premier:** Equifax, including by or through any partner, affiliate, agent, or third party, shall not use any information provided by consumers (or the fact that the consumer provided information) to enroll in TrustedID Premier to sell, upsell, or directly market or advertise its fee-based products or services.
- 18 Mandatory Training:** Equifax shall establish an information security training program that includes, at a minimum, at least annual information security training for all employees, with additional training to be provided as appropriate based on employees' job responsibilities.
- 19 Vendor Management:** Equifax shall oversee its third party vendors who have access to the Equifax Network by maintaining and periodically reviewing and revising, as needed, a Governance Process for assessing vendor compliance in accordance with Equifax's

Information Security Program to assess whether the vendor's security safeguards are appropriate for that business, which Governance Process requires vendors by contract to implement and maintain such safeguards and to notify Equifax within seventy-two (72) hours of discovering a security event, where feasible.

- 20 Incident Response Exercises:** Equifax shall conduct, at a minimum, biannual incident response plan exercises to test and assess its preparedness to respond to a security event.
- 21 Breach Notification:** Equifax shall comply with the state data breach notification laws, as applicable, and unless preempted by federal law.
- 22 Information Security Spending:** Equifax shall ensure that its Information Security Program receives the resources and support reasonably necessary for the Information Security Program to function as required by this Settlement. In addition, over a five-year period beginning 1/1/2019, Equifax shall spend a minimum of \$1B on data security and related technology.
- 23 Third-Party Assessments:** Equifax shall engage a Third-Party Assessor meeting the criteria specified in this Agreement to conduct a SOC 2 Type 2 attestation, or to conduct an assessment using industry-recognized procedures and standards in satisfaction of Regulator requirements for this Agreement (the "Third-Party Assessments"). The Third-Party Assessments will meet the following minimum standards, unless a Regulator expressly authorizes otherwise:
- a. The Third-Party Assessments will be conducted by an unbiased, independent, cybersecurity organization agreeable both to Equifax and a Regulator. Prior to selection, Equifax will disclose to the Regulator approving the Third-Party Assessor any compensated engagement by Equifax of the Third-Party Assessor in the 2 years prior to the assessment. The Third-Party Assessor shall be a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified organization; and have at least five (5) years of experience evaluating the effectiveness of computer system security or information system security.
 - b. The scope of the Third-Party Assessments, including the assertion statements required, will be established by the Third-Party Assessor in consultation with Equifax.
 - c. The Third-Party Assessments will evaluate Equifax's Information Security Program, including its policies and practices, consistent with NIST or another comparable standard.
 - d. The reporting periods for the Third-Party Assessments shall (1) cover the first 180 days following final approval of this Agreement for the initial Third-Party Assessment, and each two-year period thereafter for a total of seven (7) years. Provided, however, that the parties agree in good faith to adjust this timeline to align with Third-Party Assessments performed for Regulators to the extent that they are used to satisfy this Agreement.
 - e. The Third-Party Assessor will confirm that Equifax has complied with the terms of this Agreement.

- f. The Third-Party Assessments will identify deficiencies in Equifax's Information Security Program and, in good faith cooperation with Equifax's CISO or their designee, prioritize and establish dates by which Equifax shall remediate the deficiencies identified or implement compensating controls.
- g. Within [30] days after the close of each reporting period in Paragraph 23(d) above, the Third-Party Assessor will provide to a designated Consumer Plaintiffs' Counsel a verification of compliance with this Agreement, which includes the identification of material deficiencies and Equifax's corresponding plan pursuant to Paragraph 23(f).
- h. Equifax may use a Third-Party Assessment performed in satisfaction of obligations to government entities to meet the Third-Party Assessment requirement here, provided that the assessment complies with Paragraph 23.

24 Regulator Requirements: The Parties acknowledge that Equifax may be obligated to comply with requirements governing Equifax's Information Security Program and Third-Party Assessments as part of the resolution of claims stemming from the 2017 Data Breach and asserted against Equifax by certain government entities (the "Regulator Requirements"). In the event that any of the specific obligations set forth in the above provisions conflict with provisions set forth in the Regulator Requirements regarding the same or similar obligations, then the more restrictive Regulator provision shall apply and supersede the less restrictive provision in this Agreement.

25 Miscellaneous: In the event that technological or industry developments or intervening changes in law render any of the provisions set forth in this Agreement obsolete or make compliance by Equifax with any provision impossible or technically impractical, Equifax will provide notice to Co-Lead Counsel for Consumer Plaintiffs. If the Parties reach a mutual agreement that the elimination or modification of a provision is appropriate, they may jointly petition the Court to eliminate or modify such provision. If the Parties fail to reach an agreement, Equifax may petition the Court to eliminate or modify such provision. Under any circumstances, to the extent Consumer Plaintiffs believe that Equifax is not complying with any business practices commitments, they will first meet and confer with Equifax prior to seeking relief from the Court.

EXHIBIT C

Class Counsel's August 1, 2019 Public Statement

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

**STATEMENT OF CLASS COUNSEL
IN THE EQUIFAX DATA BREACH CONSUMER CLASS ACTION**

August 1, 2019

This statement by former Georgia Governor Roy Barnes of Marietta, Georgia; Ken Canfield of Atlanta, Georgia; Amy Keller of Chicago, Illinois; and Norman Siegel of Kansas City, Missouri: responds to misinformation circulating regarding the recently announced Equifax data breach settlement.

On July 22, 2019, a federal judge in Atlanta preliminarily approved a class action settlement resolving all consumer claims from the 2017 Equifax data breach settlement. The settlement is historic, requires Equifax to pay much more than in any previous data breach case, and provides relief to all consumers who were harmed. Here is a broad outline of the available relief:

- (1) Class members may claim up to \$20,000 in actual losses from identity theft and costs incurred protecting themselves from future harm. All class members who purchased credit monitoring services as a result of the Equifax data breach may claim the cost as an actual out of pocket loss.
- (2) Class members get 10 years of free credit monitoring. Class members who prefer to keep their own monitoring service and meet other conditions are entitled to an alternative cash payment subject to an overall cap of \$31 million.
- (3) Class members have access to free identity restoration services for 7 years, whether or not they make a claim.
- (4) All class members will benefit from requirements that Equifax overhaul its systems and Equifax must spend at least \$1 billion over 5 years on cybersecurity measures.

In choosing what benefits are best for them, we urge class members to only rely on the official notice approved by the court, not media stories or social media posts. The official notice and answers to frequently asked questions can be found at www.equifaxbreachsettlement.com.

A more detailed response follows:

We reached a settlement with Equifax to resolve all consumer class action lawsuits on March 30, 2019. Equifax's board approved the settlement the next day. The settlement was later revised at the request of federal and state regulators. Many of its terms were later incorporated into 52 separate consent orders between Equifax, the FTC, CFPB, and State and Territorial Attorneys General.

On the morning of July 22, before we even presented the class action settlement to the court, a deluge of pervasive media coverage began that has caused much confusion and misinformation. Many media reports wrongly suggested all class members are entitled to \$125, triggering a flood

of \$125 claims on the settlement website. Many of those claims are not valid and will be rejected by the settlement administrator.

A valuable component of the class action settlement is ten years of free credit monitoring, which would cost each class member nearly \$2,000 if purchased at retail. That monitoring provides services that are tailored to the exact breach that happened here—including dark web scanning for social security numbers—and, when combined with freezing your credit, is the best way that consumers can protect themselves from fraud or identity theft.

The settlement does not limit the number of class members who can sign up for credit monitoring. Every single class member who chooses credit monitoring will have the entire cost paid by Equifax. If more than 7 million class members sign up, Equifax will have to pay more money into the fund. The ultimate cost to Equifax if all 147 million class members sign up exceeds \$2 billion.

The cash payment of up to \$125 is meant to provide an “alternative” benefit to class members who prefer the credit monitoring service they already have. For that reason, the only class members eligible for the alternative benefit are those who already have monitoring, certify they intend to keep it for at least six months, and name the company that provides the service.

The alternative payments are capped at \$31 million to ensure sufficient funds are available to pay for class members’ out of pocket losses. At the end of the claims period, if money is left over after those out of pocket losses are paid, the cap will be lifted and much of the additional money will be distributed to those who claimed the alternative cash payment.

Until the claims deadlines expire, we will not know how much class members who have chosen the alternative cash payment will get. That will depend on the number of claims, how many claims are valid, and whether the cap will be lifted. But, if current trends continue, we expect class members will get substantially less than \$125. Eligible class members who have not yet decided between credit monitoring and a cash payment should keep that in mind when they make their choice. Those who have already chosen cash will be given an opportunity to reconsider their choice and file a new or amended claim.

Although class actions still remain the best way for consumers to obtain relief when impacted by a data breach, this settlement demonstrates that stronger laws need to be passed to protect consumers and ensure that they are fully compensated when corporations do not adequately protect their private information.

#####

EXHIBIT D

Chart of Hours and Lodestar by Firm

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

TIME SUMMARY FOR INCEPTION TO SEPTEMBER 30, 2019		
Firm	Total by Firm	Total by Firm
	Hours	Lodestar
<u>Court Appointed Leadership</u>		
Barnes Law Group, LLC	3,164.10	\$1,807,848.50
Cohen Milstein Sellers & Toll, PLLC	1,444.50	\$980,137.00
DiCello Levitt Gutzler	4,275.80	\$3,004,355.00
Doffermyre Shields Canfield & Knowles, LLC	2,873.60	\$2,873,600.00
Doss Firm, LLC	1,141.80	\$720,030.00
Evangelista Worley LLC	608.80	\$372,600.00
Gibbs Law Group LLP	2,305.10	\$1,282,741.50
Griffin & Strong P.C.	221.70	\$92,965.00
Hausfeld LLP	2,274.60	\$1,286,259.00
Milberg Tadler Phillips Grossman LLP	1,661.30	\$1,158,597.50
Tadler Law LLP	14.20	\$11,530.00
Morgan & Morgan Complex Litigation Group	1,604.60	\$1,230,361.30
Murphy, Falcon & Murphy	839.80	\$544,064.50
Stueve Siegel Hanson LLP	6,444.20	\$4,592,801.00
<u>Other Consumer Counsel</u>		
Ahdoot & Wolfson	19.70	\$10,697.50
Alexander Schack	26.60	\$9,830.00
Barrack, Rodos & Bacine	3.00	\$2,310.00
Berger & Montague P.C.	53.70	\$35,289.50
Blood, Hurst & O'Reardon LLP	73.80	\$39,031.00
Buether Joe & Carpenter, LLC	5.40	\$2,767.50
Christensen Young & Associates	18.20	\$10,920.00
Colson Hicks Eidson	7.30	\$4,560.00
Consumer Justice Center	19.90	\$8,955.00
David A. Bain, LLC	23.60	\$12,036.00
Dorros Law	4.20	\$2,520.00
Eggnatz Pascucci	13.70	\$7,192.50
Emerson Firm, PLLC	8.90	\$7,075.50
Emerson Scott LLP	44.90	\$35,695.50
Federman & Sherwood	60.40	\$51,040.00
Fink Bressack	23.60	\$15,056.00
Finkelstein & Thompson	29.90	\$21,965.00
Fleming Law Firm, PLLC	20.90	\$10,697.50
Geragos & Geragos, APC	96.10	\$61,665.00

TIME SUMMARY FOR INCEPTION TO SEPTEMBER 30, 2019		
Firm	Total by Firm	Total by Firm
	Hours	Lodestar
Goldman Scarlato & Penny, P.C.	67.70	\$48,407.50
Grabar Law Office	22.60	\$17,515.00
Green & Noblin P.C.	4.20	\$1,424.00
Gustafson Gluek PLLC	159.40	\$93,295.00
Hannon Law Firm, LLC	120.40	\$22,084.00
Harris Lowry Manton	9.50	\$3,325.00
Hellmuth & Johnson	22.70	\$18,704.50
Kantrowitz, Goldhamer & Graifman, P.C.	22.10	\$18,785.00
Keller Rohrback	95.80	\$44,721.50
Levi & Korsinsky, LLP	24.70	\$19,786.00
Daniel Mirarchi, Esq.	4.00	\$2,340.00
Mastando & Artrip, LLC	21.10	\$9,495.00
NastLaw LLC	29.20	\$21,112.00
O'Brien Law Firm	10.10	\$6,565.00
Quinn, Connor, Weaver, Davies & Rouco	7.40	\$4,215.00
Robbins Arroyo	17.50	\$7,952.50
Saltz, Mongeluzzi, Barrett & Bendesky, P.C.	13.50	\$7,222.50
Sanford Heisler Sharp, LLP	519.80	\$106,274.00
Saveri & Saveri, Inc.	7.00	\$3,640.00
Scott Cole & Associates, APC	11.00	\$6,350.50
Spector Roseman & Kodroff, PC	14.80	\$9,339.00
Stritmatter Kessler Whelan Koehler Moore	158.00	\$63,030.00
Stull, Stull & Brody	55.70	\$52,137.50
The Miller Law Firm	108.50	\$52,911.00
Webb, Klase & Lemond, LLC	28.10	\$15,092.50
Wilentz, Goldman & Spitzer, P.A.	22.70	\$18,727.50
Withers Bergman LLP	6.50	\$4,712.50
TOTAL FOR LEADERSHIP	28,874.10	\$19,957,890.30
TOTAL FOR NON-LEADERSHIP	2,137.80	\$1,028,467.50
TOTAL ALL FIRMS	31,011.90	\$20,986,357.80

EXHIBIT E

Chart of Hourly Rates by Timekeeper

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

Firm	Timekeeper	Position	Rate	License Year
Barnes Law Group, LLC	Tribble, Cam	Partner	\$600.00	2007
Barnes Law Group, LLC	Rosichan, Ben	Associate	\$350.00	2017
Barnes Law Group, LLC	Barnes, Roy	Partner	\$1,050.00	1972
Barnes Law Group, LLC	Bevis, John	Partner	\$675.00	1996
Barnes Law Group, LLC	Bartholomew, John	Associate	\$400.00	2009
Barnes Law Group, LLC	O'Neill, Kelsey	Paralegal	\$165.00	N/A
Berger & Montague P.C.	Lambira, Jon	Partner	\$635.00	2003
Cohen Milstein Sellers & Toll, PLLC	Friedman, Andrew, N.	Partner	\$940.00	1983
Cohen Milstein Sellers & Toll, PLLC	Handmaker, Sally	Associate	\$570.00	2011
Cohen Milstein Sellers & Toll, PLLC	Wozniak, Mariah	Paralegal	\$300.00	N/A
Cohen Milstein Sellers & Toll, PLLC	Hamdan, Shireen	Paralegal	\$290.00	N/A
DiCello Levitt Gutzler	Keller, Amy	Partner	\$750.00	2008
DiCello Levitt Gutzler	Levitt, Adam	Partner	\$985.00	1993
DiCello Levitt Gutzler	Hawal, Justin	Associate	\$500.00	2014
DiCello Levitt Gutzler	Abramowitz, Mark	Associate	\$550.00	2011
DiCello Levitt Gutzler	Seese, Caitlin	Paralegal	\$250.00	N/A
DiCello Levitt Gutzler	Lebdjiri, Audree	Paralegal	\$300.00	N/A
Doffermire Shields Canfield & Knowles, LLC	Canfield, Kenneth	Partner	\$1,000.00	1977
Doffermire Shields Canfield & Knowles, LLC	Doffermire, Everette	Partner	\$1,000.00	1973
Doss Firm, LLC	Doss, Jason	Partner	\$650.00	2002
Doss Firm, LLC	Doss, Joy	Partner	\$600.00	2002
Doss Firm, LLC	Brannan, Sam	Partner	\$600.00	1990
Evangelista Worley, LLC	Worley, David J.	Partner	\$750.00	1985
Evangelista Worley, LLC	Kaltman, Barry	Paralegal	\$225.00	N/A
Evangelista Worley, LLC	Toran, Leslie	Counsel	\$650.00	2004
Evangelista Worley, LLC	McGregor, Kristi Stahnke	Partner	\$725.00	1999
Federman & Sherwood	Federman, William	Partner	\$850.00	1982
Geragos & Geragos, APC	Feldman, Lori	Associate	\$650.00	1991
Gibbs Law Group LLP	Berger, David	Partner	\$675.00	2008
Gibbs Law Group LLP	Blumenthal, Aaron	Associate	\$430.00	2016
Gibbs Law Group LLP	Gibbs, Eric	Partner	\$910.00	1995
Gibbs Law Group LLP	Schwartzberg, Nicole	Associate	\$410.00	2013
Gibbs Law Group LLP	Khamvongsa, Mani	Associate	\$375.00	2008
Gibbs Law Group LLP	Karl, Amanda	Associate	\$415.00	2014
Gibbs Law Group LLP	Stein, Dave	Partner	\$605.00	2008
Gibbs Law Group LLP	Attar, Natalie	Paralegal	\$225.00	N/A
Gibbs Law Group LLP	Lopez, Steve	Associate	\$415.00	2014
Gibbs Law Group LLP	Mura, Andre	Partner	\$635.00	2005
Gibbs Law Group LLP	Grille, Simon	Associate	\$500.00	2013
Gibbs Law Group LLP	Bloomfield, Joshua	Associate	\$540.00	2001
Goldman Scarlato & Penny, P.C.	Goldman, Mark S.	Partner	\$725.00	1986
Griffin & Strong P.C.	Maher, David	Partner	\$400.00	1993
Griffin & Strong P.C.	Strong, Rodney	Partner	\$450.00	1989
Gustafson Gluek PLLC	Dennis, Kaitlyn L.	Associate	\$400.00	2015
Hannon Law Firm, LLC (The)	Dunlap, Madelyn	Legal Assistant	\$95.00	N/A
Hausfeld LLP	Nathan, Steven	Counsel	\$600.00	1987
Hausfeld LLP	Pizzirusso, Jamie J.	Partner	\$770.00	2001
Hausfeld LLP	Derksen, Samantha	Associate	\$400.00	2018
Hausfeld LLP	McCune, Kenya	Paralegal	\$280.00	N/A
Hausfeld LLP	Engdahl, Ian	Associate	\$400.00	2019
Hausfeld LLP	Kim, Jane	Law Clerk	\$260.00	N/A
Keller Rohrback	Montgomery, Mary	Paralegal	\$325.00	N/A
Milberg Tadler Phillips Grossman LLP	Clark, Melissa	Partner	\$725.00	2008
Milberg Tadler Phillips Grossman LLP	Tadler, Ariana J.	Partner	\$925.00	1992
Milberg Tadler Phillips Grossman LLP	McKenna, Elizabeth	Counsel	\$625.00	1999
Milberg Tadler Phillips Grossman LLP	Joseph, Jason A.	Paralegal	\$325.00	N/A
Milberg Tadler Phillips Grossman LLP	Rado, Andrei	Partner	\$650.00	2000

Milberg Tadler Phillips Grossman LLP	de Bartolomeo, AJ	Partner	\$875.00	1988
Milberg Tadler Phillips Grossman LLP	Burse, W. S.	Investigator	\$550.00	N/A
Milberg Tadler Phillips Grossman LLP	Kelston, Henry J.	Partner	\$700.00	1979
Morgan & Morgan Complex Litigation Group	Yanchunis, John	Partner	\$950.00	1981
Morgan & Morgan Complex Litigation Group	Glassman, Marisa	Associate	\$636.00	2009
Morgan & Morgan Complex Litigation Group	Barthle, Patrick	Associate	\$658.00	2012
Morgan & Morgan Complex Litigation Group	McGee, Ryan	Associate	\$742.00	2009
Morgan & Morgan Complex Litigation Group	Walters, Lee	Investigator	\$300.00	N/A
Morgan & Morgan Complex Litigation Group	Reign, David	Investigator	\$300.00	N/A
Murphy, Falcon & Murphy	Murphy III, William H.	Partner	\$895.00	1994
Murphy, Falcon & Murphy	Meeder, Jessica	Partner	\$670.00	2005
Murphy, Falcon & Murphy	Grimes, Saidah	Associate	\$280.00	2014
Murphy, Falcon & Murphy	Tranter, Matthew	Associate	\$250.00	2015
Murphy, Falcon & Murphy	Zerhouni, William	Partner	\$735.00	2003
Murphy, Falcon & Murphy	Thornton, Heather	Paralegal	\$185.00	N/A
Sanford Heisler Sharp, LLP	Martinez, Adan	Associate	\$212.50	2018
Sanford Heisler Sharp, LLP	Sheenan, Claire	Paralegal	\$147.50	N/A
Sanford Heisler Sharp, LLP	Krupp, Amber	Paralegal	\$147.50	N/A
Sanford Heisler Sharp, LLP	Velkovsky, Pavel	Paralegal	\$137.50	N/A
Stritmatter Kessler Whelan Koehler Moore	Laird, Jeanne	Paralegal	\$275.00	N/A
Stritmatter Kessler Whelan Koehler Moore	Fleming, Catherine	Partner	\$550.00	2008
Stueve Siegel Hanson	Siegel, Norman	Partner	\$935.00	1993
Stueve Siegel Hanson	Vahle, Barrett	Partner	\$745.00	2004
Stueve Siegel Hanson	Moore, Austin	Associate	\$575.00	2011
Stueve Siegel Hanson	Campbell, Michelle	Paralegal	\$275.00	N/A
Stueve Siegel Hanson	Smith, Emily	Associate	\$425.00	2014
Stueve Siegel Hanson	Williams, Sheri	Paralegal	\$225.00	N/A
Stueve Siegel Hanson	Hickey, David	Associate	\$525.00	2009

EXHIBIT F

Chart of Expenses by Category

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

EXPENSE SUMMARY	
Category	Total
Federal Express, Local Courier, Postage	\$6,701.47
Hotels	\$90,474.21
Meals	\$29,879.40
Air Travel	\$129,988.63
Discovery Costs	\$25,102.06
Pacer, Electronic Research	\$167,808.19
Experts	\$466,408.16
Court Fees	\$52,900.66
Process Service	\$9,058.30
Hearing Transcripts	\$6,812.85
Ground Transportation (Mileage, Rental Car, Parking, Taxi, Rideshare)	\$28,647.23
Miscellaneous	\$104,493.55
Mediation Services	\$129,758.75
TOTAL	\$1,248,033.46

EXHIBIT G

List of Settlement Class Representatives

In re: Equifax Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Class Counsel's Supplemental Declaration in Support of
Plaintiffs' Motion for Attorneys' Fees, Expenses, and
Service Awards to the Class Representatives

1. Cheyra Acklin-Davis
2. Christy Adams
3. Robert Anderson
4. Donald Angelechio
5. Michele Renee Archambault
6. Dean Edward Armstrong
7. Justin Bakko
8. Robert Benson
9. David Bielecki
10. Michael Aaron Bishop
11. Sabina Bologna
12. Nancy Rae Browning
13. Francine Campbell
14. Mark Carr
15. Natasha Carr
16. Michael Chase
17. Jack Cherney
18. Grace Cho
19. Ricardo A. Clemente
20. Bridgette Craney
21. Thomas Edward Crowell
22. Germany Davis
23. Christopher P. Dunleavy
24. Abby Lee Elliott
25. Robert J. Etten
26. Kayla Ferrel
27. Janelle Ferrell
28. Larry Frazier
29. Andrew Galpern
30. James Gay
31. Michael Getz
32. Terry Goza
33. Thomas E. Greenwood
34. Josh Grossberg
35. Jasmine Guess
36. John R. Hammond

37. Thomas W. Hannon
38. Jennifer Ann Harris
39. Kismet Harvey
40. Todd Heath
41. Bob Helton
42. Margaret M. Henkel
43. Cathy Louise Henry
44. Alexander Hepburn
45. Eva Hitchcock
46. Kathleen Holly
47. Michael Louis Hornblas
48. Gregory Jacobs
49. David L. Kacur
50. Aloha Kier
51. Brenda King
52. Alvin Alfred Kleveno Jr.
53. Joanne Klotzbaugh
54. Emily Knowles
55. Debra Lee
56. Brett D. Lemmons
57. Leah Lipner
58. Maria Martucci
59. Delitha J. May
60. James McGonnigal
61. Anthony Mirarchi
62. Barry Napier
63. Justin O'Dell
64. Kyle Olson
65. Mel C. Orchard III
66. Joseph Packwood
67. John J. Pagliarulo
68. Richard Dale Parks
69. Clara Parrow
70. Bruce Pascal
71. Sylvia Patterson
72. Wanda Paulo

73. Dallas Perkins
74. Stephen Plante
75. Gregg Podalsky
76. Sanjay Rajput
77. Benjamin Sanchez
78. David Sands
79. Rodd Santomauro
80. Maria Schifano
81. Thomas Patrick Schneider
82. James David Sharp
83. Miche' Sharpe
84. John Simmons II
85. Amie Louise Smith
86. Anna Solorio
87. Jonathan Strausser
88. Kim Strychalski
89. Pete Swiftbird
90. Cheryl Ann Tafas
91. Tabitha Thomas Hawkins
92. Gerry Tobias
93. Nathan Alan Turner
94. Jennifer J. Tweeddale
95. Katie Van Fleet
96. Richard Whittington II