JOSEPH SAVERI LAW FIRM, LLP
Joseph R. Saveri (SBN 130064)
Cadio Zirpoli (SBN 179108)
Christopher K.L. Young (SBN 318371)
Kevin E. Rayhill (SBN 267496)
601 California Street, Suite 1505
San Francisco, CA 94108
Tel (415) 500-6800
jsaveri@saverilawfirm.com
czirpoli@saverilawfirm.com
cyoung@saverilawfirm.com
krayhill@saverilawfirm.com

KOZYAK TROPIN & THROCKMORTON, LLP
Robert Neary (Fla. Bar No. 81712, *Pro Hac Vice Forthcoming*)
Benjamin Widlanski (Fla. Bar No. 1010644, *Pro Hac Vice Forthcoming*)
Gail McQuilkin (Fla. Bar No. 969338, *Pro Hac Vice Forthcoming*)
Daniel Herrera (Fla. Bar No. 1048643, *Pro Hac Vice Forthcoming*)
2525 Ponce de Leon Blvd., Floor 9
Coral Gables, FL 33134
Tel (305) 372-1800
rn@kttlaw.com
bwidlanski@kttlaw.com
gam@kttlaw.com
dherrera@kttlaw.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

MEGAN JOSEPH, on behalf of her minor children, B.J. and C.J., and EMILY KIDDER and DALE KIDDER, on behalf of their minor children, E.K. and M.K., and all other similarly situated individuals,

Plaintiffs,

v.

POWERSCHOOL HOLDINGS, INC. and POWERSCHOOL GROUP, LLC,

Defendants.

Case No:

COMPLAINT FOR:

(1) Negligence
(2) Negligence Per Se
(3) Unjust Enrichment
(4) Invasion of Privacy
(5) Violation of the California Unfair Competition Law (Cal. Bus. & Prof. Code §17200 et seq.)

DEMAND FOR JURY TRIAL

CLASS ACTION

TABLE OF CONTENTS

Plaintiffs Megan Joseph, on behalf of her minor children B.J. and C.J., and Emily Kidder and Dale Kidder, on behalf their minor children, E.K. and M.K., and all similarly situated individuals (the "Class Members" or the "Class," defined below), bring this action against PowerSchool Holdings, Inc. and PowerSchool Group, LLC, (collectively, "PowerSchool") and allege as follows:

I. SUMMARY OF THE CASE

1. PowerSchool is a leading provider of cloud-based software for K-12 education in the United States. PowerSchool collects and maintains highly sensitive personal identifiable information ("PII") for more than 60 million students, parents, and school faculty worldwide. PowerSchool acquires this PII through its education technology products, which it sells to schools and school districts.

2. On or around December 28, 2024, PowerSchool lost control of this PII when it was stolen by cybercriminals who, because of PowerSchool's negligent website design and lack of modern cybersecurity protections, accessed the PII via a compromised login (the "Data Breach").

3. The Data Breach differs from typical data breaches because it affects consumers who had no relationship with PowerSchool and never consented to PowerSchool collecting and storing their PII.

4. Upon information and belief, cybercriminals gained unauthorized access to PII held by PowerSchool including names, birth dates, addresses, parent/guardian names, and parent/guardian phone numbers, tax information numbers, as well as private health information such as medical conditions and allergies.

5. In early January 2025, PowerSchool began notifying customers that their data was impacted and that most of the PII accessed in the Data Breach included sensitive information pertaining to students under the age of 18.

6. PowerSchool failed to maintain reasonable security safeguards and protocols to protect its users' PII—none of the information accessed in the Data Breach was encrypted. PowerSchool also lacked proper controls to determine which students, parents, and faculty were impacted by the Data Breach.

7. PowerSchool's failure to timely detect and report the Data Breach caused Plaintiffs and Class Members to be vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII. Even when PowerSchool finally notified

Plaintiffs and Class Members of their PII exfiltration, PowerSchool failed to adequately describe the Data Breach and its effects, as well as the measures it took to prevent data breaches from occurring in the future.

8. In failing to adequately protect consumers' information, failing to adequately notify them about the breach, and obfuscating the nature of the breach, PowerSchool violated state and federal laws and harmed thousands of its current and former consumers.

9. Plaintiffs and Class Members are victims of PowerSchool's negligence and inadequate cyber security measures. Plaintiffs and Class Members trusted PowerSchool with their PII. But PowerSchool betrayed that trust by failing to use up-to-date security practices to prevent the Data Breach.

10. Plaintiffs' minor children are also Data Breach victims.

11. Accordingly, Plaintiffs bring this lawsuit seeking damages and injunctive relief to remediate PowerSchool's security failures, credit monitoring or repair services to protect Class Members, and reasonable attorneys' fees and costs.

II. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. PowerSchool and at least one Class Member are citizens of different states. There are over 100 putative Class Members.

13. This Court has personal jurisdiction over PowerSchool Holdings and PowerSchool Group because both entities are headquartered in this state, have their principal place of business in this state, and conduct substantial business in this state. PowerSchool Holdings and PowerSchool Group have also conducted systematic and continuous activities in California; and there is a substantial nexus between the conduct PowerSchool directs at California and the claims asserted herein.

14. Venue is proper in this Court because all Defendants reside in this state and this district and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this district. *See* 28 U.S.C. § 1391(b)(2).

III. PARTIES

15. Plaintiff Megan Joseph is an individual and the mother and legal guardian of B.J. and C.J. At all relevant times, Ms. Joseph has been domiciled in North Carolina.

16. B.J. is a minor under the age of 18. At all relevant times, she has been domiciled in the state of North Carolina. B.J. attends school at Valle Crucis School, an elementary school within the Watauga County School District.

17. C.K. is a minor under the age of 18. At all relevant times, she has been domiciled in the state of North Carolina. C.J. attends school at Valle Crucis School, an elementary school within the Watauga County School District.

18. Plaintiffs Emily Kidder and Dale Kidder, a married couple, are the mother and father and legal guardians of E.K. and M.K. At all relevant times, the Kidders have been domiciled in North Carolina.

19. E.K. is a minor under the age of 18. At all relevant times, she has been domiciled in the state of North Carolina. E.K. attends school at Mabel Elementary School, an elementary school within the Watauga County School District.

20. M.K. is a minor under the age of 18. At all relevant times, he has been domiciled in the state of North Carolina. M.K. attends school at Watauga High School, a high school within the Watauga County School District.

21. The Watauga County School District has used PowerSchool products that store student data. As a result, B.J's, C.J.'s, E.K.'s, and M.K.'s PII was collected or likely collected by PowerSchool and their PII was accessed in the Data Breach.

22. Defendant PowerSchool Holdings, Inc. is a Delaware corporation with its principal place of business at 150 Parkshore Drive, Folsom, California 95630.

23. Defendant PowerSchool Group, LLC is a Delaware limited liability company with its principal place of business at 150 Parkshore Drive, Folsom, California 95630.

24. Upon information and belief, each Defendant was a principal, agent, alter ego, joint venture partner, partner, or affiliate of each other, and in doing the acts alleged herein, was acting within the course and scope of that principal, agent, alter ego, joint venture, partnership, or affiliate relationship. Each Defendant (1) had actual knowledge of the wrongful acts of the other; (2) ratified, approved, joined in, acquiesced, or authorized the wrongful acts of each other; and (3) retained the benefits of those wrongful acts.

IV. FACTUAL BACKGROUND

PowerSchool

25. PowerSchool is the largest provider of cloud-based education software for K-12 education in the U.S., serving more than 75% of students in North America. PowerSchool's software is used by over 16,000 customers to support more than 50 million students in the United States. PowerSchool offers a full range of services to help school districts operate, including platforms for enrollment, communication, attendance, staff management, learning systems, analytics, and finance.

26. Touting an annual revenue of $697.65 million[1], PowerSchool boasts that it is "a leading provider of cloud-based software for K-12 education in North America."[2]

27. Due to the nature of its business, PowerSchool receives and maintains PII for millions of students, parents, and school faculty across the country. Specifically, PowerSchool retains the PII of students, parents, and teachers, including, but not limited to, names, addresses, social security numbers, medical information and grade information. These records were, and continue to be, stored on PowerSchool's computer systems.

28. Under state and federal law, PowerSchool had a duty to protect the PII of current and former students and school faculty members, including under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the California Consumer Protection Act of 2018 (the "CCPA"), Cal. Civ. Code § 1798, *et seq.* PowerSchool likewise had a duty to alert students, parents, and school faculty that their PII was accessed by an unauthorized third party, and was exposed.

29. PowerSchool understood the need to protect consumers' PII and prioritize its data security. In fact, PowerSchool's Privacy Policy specifically acknowledges that "PowerSchool does not own or control Student Data, which belongs to the student and/or the Customer (schools, school districts, and higher education institutions) that contracts with PowerSchool to provide access to PowerSchool Products."[3] Therefore, PowerSchool claims to "employ[] a variety of physical, administrative, and

---

[1] Stock Analysis, https://stockanalysis.com/stocks/pwsc/revenue/ (last visited January 20, 2025).
[2] Linkedin, PowerSchool, https://www.linkedin.com/company/powerschool-group-llc/ (last visited January 20, 2025).
[3] https://www.powerschool.com/privacy/ (last visited January 20, 2025).

technological safeguards designed to protect [customer] data against loss, misuse, and unauthorized access or disclosure."[4]

30. In the Global Privacy Statement on its website, PowerSchool also tell users that it is "committed to protecting [users'] personal information" and that it "endeavors to align its privacy and security operations to best practices and relevant international regulations."[5] As demonstrated below, PowerSchool does no such thing.

The Data Breach

31. On or about December 28, 2024, hackers successfully breached PowerSchool's customer support portal, PowerSource. The cybercriminals gained access to PowerSchool's Student Information System ("SIS") database through PowerSource using compromised credentials due to PowerSchool's lack of robust authentication and lack of access control security measures. The cybercriminals then used maintenance access channels to access data stored on PowerSchool's servers.

32. PowerSchool's SIS contains student, parent, and faculty PII. Hackers were able to access and steal this information by exporting the "Students" and "Teachers" database tables from PowerSchool's SIS to a .CSV file. In this way, the hackers were able to access highly-sensitive student, parent, and faculty PII such as: names; home addresses; Social Security numbers; phone numbers; email addresses; medical information; grades and grade point averages; bus stops for students; passwords for student portals; notes and alerts concerning students; student IDs; and PII of parents or guardians of students.

33. Plaintiffs' and Class Members' PII have inherent value. Cybercriminals routinely sell and trade such information on the dark web. Upon information and belief, the hackers will exploit the PII obtained in the Data Breach for profit.

34. As a direct result of the Data Breach, Plaintiffs' and Class Members' PII will likely fall into the hands of criminals or organizations that can use the detailed PII for, among other things, identity theft, fake medical insurance claims, filing fraudulent tax returns, access to prescriptions for resale, and

---

[4] *Id.*
[5] *Id.*

other medical and financial fraud. To be sure, cybercriminals can now easily access the PII and/or financial information of Plaintiffs and Class Members.

The Data Breach was a Foreseeable Risk to PowerSchool

35. As part of its core businesses, PowerSchool collects highly personal data for tens of millions of students, parents, and school faculty and generates hundreds of millions of dollars annually through the collection, storage, and use of this information. PowerSchool therefore had ample resources and a strong motive to adopt reasonable protections. PowerSchool also should have known that such protections were necessary given the value of the highly personal information it stores.

36. It is well known that PII is an invaluable commodity and a frequent target of hackers. For example, in 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[6]

37. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[7]

38. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued warnings to potential targets, so they can take appropriate measures to prepare for such attacks.[8]

39. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware

---

[6] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-ofdata-breaches-reported-in-2021-new-report-says/ (last visited January 20, 2025).

[7] *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited January, 20, 2025).

[8] *See, e.g.*, *Official Alerts & Statements – FBI*, Stop Ransomware, https://www.cisa.gov/stopransomware/official-alerts-statements-fbi (last visited January 20, 2025); US Secret Service Warns of Attacks on MSPs, Bitdefender, https://www.bitdefender.com/en-us/blog/businessinsights/us-secret-service-warns-of-attacks-on-msps.

tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[9]

40. Additionally, education technology providers similar to PowerSchool have been subject to data breaches in the past.[10]

41. Given the widespread knowledge about the risks of cyberattacks and data breaches, PowerSchool had constructive knowledge that it would almost certainly be the target of hackers. Specifically, PowerSchool knew or should have known that: (i) ransomware actors were targeting entities such as PowerSchool; (ii) ransomware gangs are ferocious in their pursuit of entities such as PowerSchool; and (iii) ransomware gangs seek to sell customer data on dark web portals.

42. Simply put, there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, sold, and published as the result of a cyberattack.

PowerSchool's Failure to Adopt Reasonable Systems and Protections

43. Despite ample warnings of possible cybersecurity threats—and the promises on its website to safeguard customer data—PowerSchool did not adopt reasonable data systems and protections to safeguard student, parent, and faculty PII; did not detect and prevent unauthorized access to this data; and did not identify and immediately alert users impacted by the Data Breach.

44. Upon information and belief, PowerSchool failed to take the following actions in accordance with its duty to safeguard PII: (1) adequately train its employees on cybersecurity protocols; (2) implement reasonable security measures to prevent data breaches; (3) implement reasonable security measures to detect data breaches; (4) implement reasonable security measures to comprehend the scope of data breaches; and (5) implement reasonable security measures to timely determine who was impacted by data breaches.

---

[9] *Ransomware Guide, U.S. CISA*, https://www.cisa.gov/stopransomware/ransomware-guide (last visited January 20, 2025).

[10] *See, e.g.*, *Pearson Hack Exposed Details on Thousands of U.S. Students*, Wall Street Journal, https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001 (last visited January 20, 2025).

45. PowerSchool could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiffs and Class Members, by properly training employees to recognize and prevent cybersecurity risks, and/or by implementing and following adequate retention policies to destroy the data that was no longer needed.

46. PowerSchool's use of outdated and insecure computer systems and software that are easy to hack, coupled with the failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for Plaintiffs' and Class Members' privacy, and has exposed their PII to unscrupulous operators, con artists, and criminals.

47. PowerSchool has done little to help those impacted by the Data Breach. Upon information and belief, it has offered credit monitoring services to only *some* of the victims. In any event, these services do not redress the injuries Plaintiffs and Class Members sustained to date and, at best, provide limited protection moving forward.

48. PowerSchool's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated their injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

PowerSchool Did Not Follow FTC Guidelines or Industry Standards

49. According to guidance from the FTC, businesses that collect consumer data should factor in the need for adequate data security to all business decision-making. The FTC has also provided guidance that identifies best practices for companies like PowerSchool to protect themselves against a data breach by adopting established industry standards for adequate protection against data incidents.

50. The FTC maintains a publication, Protecting Personal Information: A Guide for Business, which establishes guidelines for fundamental data security principles and practices.[11] The guidelines explain that businesses should, among other things:

a. encrypt information stored on computer networks;

b. understand their network's vulnerabilities;

[11] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed April 25, 2024).

c. implement policies to correct security problems;

d. have response plans in place to ensure an adequate and timely response to a data breach;

e. require complex passwords to navigate the systems;

f. use industry-tested security methods;

g. have monitoring systems in place to detect suspicious activity; and

h. verify that third-party service providers have reasonable security systems in place.

51. The guidelines also recommend that businesses not maintain information longer than is needed for authorization of a transaction and watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

52. PowerSchool failed to implement several of these industry standards and best practices, which directly and proximately caused the Data Breach and the injuries resulting therefrom to Plaintiffs and Class Members.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act.

54. PowerSchool's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

The Harm Suffered by Plaintiffs' Minor Children and Class Members

55. Plaintiffs' minor children and Class Members are current and former students and teachers of PowerSchool's clients (school districts or individual schools). As a condition of studying or working at the schools, PowerSchool required Plaintiffs and Class Members to disclose their PII.

56. Plaintiffs suffered actual injury and damages as a result of the Data Breach. Plaintiffs would not have provided PowerSchool with their children's PII had PowerSchool disclosed that it lacked security practices adequate to safeguard PII.

57. PowerSchool obtained, and maintains, Plaintiffs' and Class Members' PII for profit. PowerSchool, therefore, has a continuing legal duty and obligation to protect the data from unauthorized access and disclosure.

58. Based on PowerSchool's representations about its commitment to cybersecurity, Plaintiffs and Class Members trusted that a portion of the funds paid by their schools for PowerSchool products and services would be used to provide adequate cybersecurity for their PII.

59. Indeed, Plaintiffs and Class Members relied on PowerSchool to use reasonable security protocols and procedures to protect their PII. At minimum, they believed it would implement systems consistent with its stated privacy policies and applicable laws.

60. As a result of PowerSchool's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of the PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of PowerSchool and is subject to further breaches so long as PowerSchool fails to undertake the appropriate measures to protect the PII in their custody.

61. Plaintiffs and Class Members have a continuing interest in ensuring that their PII—which remains in PowerSchool's possession—be secured against future hacking attempts.

62. Stolen PII is one of the most valuable commodities on the criminal information black market. The value of Plaintiffs' and the proposed Class Members' PII on the black market is considerable.

63. Cybercriminals frequently post stolen PII directly on various "dark web" internet websites, making the information publicly available to other criminals, for a fee. Because stolen PII trades on the black market for years, cybercriminals have plenty of time to use that information for cash.

64. One example of criminals using PII for profit is the development of "Fullz" packages.[12] By cross-referencing different sources of PII, cybercriminals create dossiers of their victims that are astonishingly complete and accurate. These dossiers are known as Fullz packages.

65. Stolen PII from the Data Breach can easily be used to identify Plaintiffs' and Class Members' phone numbers, email addresses, and other identifiers. Cybercriminals can then easily sell the PII and related information to unscrupulous operators (such as illegal and scam telemarketers) and criminals over and over.

66. Upon information and belief, Plaintiffs' and Class Members' PII is being misused in this way. Such misuse is traceable to PowerSchool's inadequate cybersecurity measures which culminated in the Data Breach.

67. Plaintiffs and Class Members have spent, and will continue to spend, time and resources monitoring their data and addressing the issues caused by the Data Breach. For example, Plaintiffs and Class Members must monitor personal accounts, use credit monitoring and identify protection services, and continue to monitor information about the Data Breach.

68. Specifically, due to the Data Breach, Plaintiffs and Class Members have suffered: loss of the ability to control their PII; diminution in the value of their PII; compromise and continuing publication of their PII; out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud; the opportunity costs of the time spent trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud; unauthorized use of their stolen PII; and/or continued risk of exposure of their PII.

---

[12] *Fullz: Definition, Examples, Minimizing Risk*, Investopedia, https://www.investopedia.com/fullz-definition-4684000 (last visited January 20, 2025).

69. As a result of the Data Breach, Plaintiffs and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure.

70. Because the breached PII will likely remain available on the dark web for years to come, harm stemming from the Data Breach may not materialize for several years, Plaintiffs and Class Members must now endure years of conducting constant surveillance of their financial and personal records, and the loss of time and money that comes with this.

71. Compensating Plaintiffs and Class Members for their out-of-pocket expenses associated with the Data Breach is not sufficient to make them whole. Plaintiffs and Class Members also suffer emotional distress about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions. Such injuries go far beyond allegations of mere worry or inconvenience and are the type of personal injuries for which the law provides redress.

Plaintiffs and Class Members Face Significant Risk of Continued Identity Theft

72. The ramifications of PowerSchool's failure to keep Plaintiffs' and Class Members' PII secure are severe. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[13]

73. The PII compromised in the Data Breach is highly valuable to identity thieves because it can be used to gain access to a variety of existing accounts and websites to fraudulently convey assets, drain bank accounts or open lines of credit.

74. Identity thieves can also use the stolen data to harm Plaintiffs and Class Members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. Victims of identity theft often experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

---

[13] Anne Saita, *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited January 20, 2025).

75. In addition to these losses, which can exceed thousands of dollars, victims of identity theft have to spend a considerable amount of time repairing the damage caused by the theft of their PII. For example, those whose PII was used to open new accounts will have to spend time closing existing bank/credit accounts, opening new ones, disputing charges with creditors, and correcting fraudulent information in their credit reports while continuously monitoring their reports for future inaccuracies.

76. Further complicating the issues faced by victims of identity theft, data thieves often wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

The Plaintiffs and Their Minor Children Experienced Injuries

77. B.J., C.J., E.K., and M.K. and Class Members are current and former students, teachers, and other faculty of PowerSchool's clients (school boards or individual schools).

78. As a condition of studying or working at its customers, PowerSchool required B.J., C.J., E.K., and M.K. and Class Members to provide their PII. PowerSchool continues to maintain that PII, and has a continuing legal duty and obligation to protect it from unauthorized access and disclosure.

79. On Friday, January 10, 2025, twenty-two days after the Data Breach began and twelve days after PowerSchool became aware of the Data Brach, Plaintiffs received an email from Watauga County Schools and the North Carolina Department of Public Information regarding the Data Breach, stating that PowerSchool is working with law enforcement to monitor the dark web for any data exposure, and that impacted students will receive notification. No other details have been provided to Plaintiffs.

80. PowerSchool exposed Plaintiffs' minor children's PII to theft by cybercriminals and misuse by nefarious actors and then deprived Plaintiffs of the earliest opportunity to guard their minor children against the Data Breach's effects by failing to promptly notify them.

81. Plaintiffs do not recall ever learning that their minor children's PII was compromised in a data breach incident, other than the breach at issue in this case.

82. As a result of the Data Breach, Plaintiffs will need to spend time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the notice of Data Breach and self-monitoring their minor children's information to ensure no fraudulent activity has occurred.

83. Plaintiffs fear for their minor children's personal financial security and face uncertainty over the PII exposed in the Data Breach. Plaintiffs' anxiety because of the Data Breach goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

84. Plaintiffs' minor children suffered actual injury from the exposure of their PII—which violates their rights to privacy.

85. Plaintiffs' minor children have suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that Plaintiffs entrusted to PowerSchool, and which was compromised in and as a result of the Data Breach.

86. Plaintiffs' minor children have suffered injuries arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being placed in the hands of unauthorized third parties and possibly criminals.

87. The imminent risk to Plaintiffs' minor children is substantial. Given the minors' lack of established credit, their information can be used to create a "clean identity slate." For example, hackers can use a minor's information to take out credit cards and car loans.[14]

88. Plaintiffs' minor children remain at a present and continued risk of harm due to the exposure and potential misuse of their PII by criminal agents.

89. Plaintiffs have a continuing interest in ensuring that their minor children's PII, which, upon information and belief, remains backed up in PowerSchool's possession, is protected, and safeguarded from future breaches.

Tolling

90. Any applicable statute of limitations have been tolled by PowerSchool's knowledge and concealment of the unlawful conduct and misrepresentations alleged herein. Plaintiffs and Class Members could not have discovered PowerSchool's unlawful conduct through reasonable diligence.

---

[14] *Hackers are leaking children's data — and there's little parents can do*, https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-canrcna1926 (last visited January 28, 2025).

91. PowerSchool knowingly, actively, affirmatively and/or negligently concealed the facts alleged herein. Plaintiffs and Class Members reasonably relied on PowerSchool's concealment.

V. CLASS ACTION ALLEGATIONS

92. Plaintiffs bring this class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class: All individuals whose PII was exfiltrated or stolen in the Data Breach.

93. Specifically excluded from the Class are PowerSchool; its officers, directors or employees; any entity in which PowerSchool has a controlling interest; and any affiliate, legal representative, heir or assign of PowerSchool. Also excluded from the Class are attorneys participating in this matter and the members of his or her immediate family, any federal, state or local governmental entities, any judicial officer presiding over this action and the members of his or her immediate family and judicial staff, and any juror assigned to this action.

94. The Class Period is the full extent of the applicable limitations period, including any tolling or other equitable considerations that extend the limitations period.

95. Plaintiffs reserve the right to modify, expand, or amend the definitions of the proposed class following the discovery period and before the Court determines whether class certification is appropriate.

96. Class Identity: The Class is readily identifiable and is a class for which records should exist. Plaintiffs anticipate providing appropriate notice to each certified class in compliance with Fed. R. Civ. P. 23(c)(2)(A) and/or (B), to be approved by the Court after class certification, or pursuant to court order under Fed. R. Civ. P. 23(d).

97. Numerosity: This action satisfies the requirements of Fed. R. Civ. P. 23(a)(1). Class Members are so numerous and geographically dispersed that joinder is impracticable. Millions of Class Members had their data accessed in the Data Breach.

98. Commonality: This action satisfies the requirements of Fed. R. Civ. P. 23(a)(2) because there are questions of law and fact common to the Class, including, but not limited to:

a. Whether PowerSchool had a duty to use reasonable care in safeguarding Plaintiffs' and the Class Members' PII;

b. Whether PowerSchool breached its duty to use reasonable care with respect to the Data Breach and/or its response to the Data Breach;

c. Whether PowerSchool had reasonable systems in place to protect against and/or detect the Data Breach;

d. Whether PowerSchool had reasonable systems in place to respond to the Data Breach;

e. Whether PowerSchool's notice to Plaintiffs and Class Members was reasonable; and

f. Whether Plaintiffs and Class Members were harmed by the Data Breach.

99. Typicality: This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because Plaintiffs' claims are typical of the claims of each of the Class Members, as all Class Members were similarly affected by PowerSchool's wrongful conduct and had their information accessed in the Data Breach.

PowerSchool has acted in a manner that applies generally to Plaintiffs and all Class Members. Each Class Member has been similarly impacted by PowerSchool's failure to implement reasonable security measures to protect Class Members' PII. The relief Plaintiffs seek in this action is typical of the relief sought for the absent Class Members.

100. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class in that Plaintiffs' interests are aligned with, and not antagonistic to, those of the other members of the Class. Plaintiffs have also retained counsel competent and experienced in the prosecution of class actions and complex data privacy cases to represent them and the Class.

101. Predominance: This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3). The above-listed questions of law and fact are common to all Class Members and predominate over questions that may affect individual Class Members.

102. Superiority and Manageability: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy where joinder of all Class Members is impracticable.

103. Because the monetary damages suffered by each individual Class Member may be relatively small, the expense and burden of individual litigation would make it difficult or impossible for

individual Class Members to redress the wrongs done to each of them individually, such that most or all Class Members would have no rational economic interest in individually controlling the prosecution of specific actions. The burden imposed on the judicial system by individual litigation, and to the PowerSchool, by even a small fraction of the Class Members, would be enormous.

104. In comparison to piecemeal litigation, class action litigation presents far fewer management difficulties, far better conserves the resources of both the judiciary and the parties, and far more effectively protects the rights of each Class Member. The benefits to the legitimate interests of the parties, the court, and the public resulting from class action litigation substantially outweigh the expenses, burdens, inconsistencies, economic infeasibility, and inefficiencies of individualized litigation. Class adjudication is simply superior to other alternatives under Fed. R. Civ. P. 23(b)(3)(D).

105. Plaintiffs are unaware of any obstacles likely to be encountered in the management of this action that would preclude its maintenance as a class action. Rule 23 provides the Court with the authority and flexibility to maximize the efficiencies and benefits of the class mechanism and reduce management challenges. The Court may, on motion of Plaintiffs or on its own determination, certify a class for claims sharing common legal questions; utilize the provisions of Fed. R. Civ. P. 23(c)(4) to certify particular claims, issues, or common questions of law or of fact for class-wide adjudication; certify and adjudicate bellwether class claims; and utilize Fed. R. Civ. P. 23(c)(5) to divide any Class into subclasses.

VI. CAUSES OF ACTION

COUNT I

Negligence

106. Plaintiffs re-allege and incorporate by reference paragraphs 1-105 of the Complaint as if fully set forth herein.

107. Plaintiffs and Class Members entrusted their PII to PowerSchool based on the understanding that PowerSchool would take reasonable steps to safeguard this data. Indeed, PowerSchool collected and stored Plaintiffs and Class Members' personal information, including addresses, Social Security numbers, dates of birth, health insurance information, and personal health information including disabilities, immunization records, and medications.

108. PowerSchool owed a duty of care to Plaintiffs and Class Members to preserve and protect the confidentiality of the personal information that it collected. This duty included, among other obligations, maintaining and testing its security systems and networks, and the systems and networks of its vendors, as well as taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiffs and Class Members from unauthorized access and use.

109. PowerSchool's duties also arise by operation of statute. Pursuant to the FTC Act, 15 U.S.C. § 45, PowerSchool had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

110. It was foreseeable that any failure by PowerSchool to adopt adequate security systems consistent with industry standards would increase the risk that Plaintiffs' and Class Members' PII would be accessed by cybercriminals in a data breach. PowerSchool knew or should have known that Plaintiffs' and Class Members' PII was an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States.

111. As the nation's leading provider of cloud-based software for K-12 education, PowerSchool has full knowledge of the sensitivity of the PII at issue in this case and the harm that unauthorized access can cause for Plaintiffs and Class Members.

112. PowerSchool owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals that PowerSchool knew or should have known would suffer injury-in-fact from PowerSchool's inadequate security practices and systems.

113. PowerSchool owed Plaintiffs and Class Members at least the following duties:

a. to exercise reasonable care in handling and using the PII in its care and custody;

b. to implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized; and

c. to notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their PII.

114. Therefore, PowerSchool owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. Plaintiffs and Class Members needed PowerSchool to take appropriate measures to timely protect their PII, to be vigilant in the face of

an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

115. PowerSchool also had a duty to exercise appropriate clearinghouse practices to remove PII when it was no longer necessary to retain it under applicable regulations.

116. PowerSchool knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and Class Members involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

117. PowerSchool's duty to use reasonable security measures arose because of the special relationship that existed between PowerSchool, on the one hand, and Plaintiffs and Class Members, on the other hand. That special relationship arose because Plaintiffs and Class Members entrusted PowerSchool with their PII, which is a necessary part of PowerSchool's products and services.

118. Under the FTC Act, 15 U.S.C. § 45, PowerSchool had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

119. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as PowerSchool, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of PowerSchool's duty to protect Plaintiffs and the Class Members' sensitive PII.

120. PowerSchool violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. PowerSchool's conduct was particularly unreasonable given the nature and amount of PII PowerSchool had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals, such as Plaintiffs and Class Members, in the event of a breach, which ultimately came to pass.

121. The risk that unauthorized persons would attempt to gain access to the PII at issue here and misuse it was foreseeable. PowerSchool stores vast amounts of valuable data for students, parents, and school faculty. Similar education technology providers had been subject to data breaches in previous

years. PowerSchool also alerted the FBI that it was the target of a data theft campaign in the period before the Data Breach. Therefore, it was foreseeable that unauthorized individuals would attempt to access PowerSchool's databases—whether by malware or otherwise.

122. The PII at issue is highly valuable, and PowerSchool knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

123. PowerSchool acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII by:

a. enabling access to this information by third parties through negligent website design; and

b. failing to properly supervise the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

124. PowerSchool also breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members. Indeed, PowerSchool has admitted that the PII of Plaintiffs and the Class was wrongfully accessed, and/or disclosed to unauthorized third persons because of the Data Breach.

125. PowerSchool further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach.

126. PowerSchool's negligence and failure to exercise reasonable care directly and proximately caused actual, tangible, injury-in-fact and damages for Plaintiffs and Class Members, including the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by PowerSchool's negligence.

COUNT II

Negligence Per Se

127. Plaintiffs re-allege and incorporate by reference paragraphs 1-105 of the Complaint as if fully set forth herein.

128. Under the FTC Act, PowerSchool had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. § 45.

129. Moreover, Plaintiffs' and Class Members' injuries are precisely the type of injuries that the FTC Act guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that PowerSchool inflicted upon Plaintiffs and Class Members.

130. PowerSchool's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because PowerSchool is bound by industry standards to protect confidential PII.

131. PowerSchool violated its duties and its obligations under the FTC Act by reason of the failures that led to the Data Breach.

COUNT III

Unjust Enrichment

132. Plaintiffs re-allege and incorporate by reference paragraphs 1-105 of the Complaint as if fully set forth herein.

133. Plaintiffs and Class Members conferred a monetary benefit on PowerSchool when PowerSchool's clients provided Plaintiffs' and Class Members' PII to PowerSchool, which PowerSchool collected, maintained, and used for profit.

134. PowerSchool willingly retained that benefit, knowing that it could use Plaintiffs' and Class Members' PII for financial gain.

135. Plaintiffs and Class Members (or their third-party agents) reasonably understood that PowerSchool would use adequate cybersecurity measures to protect the PII that they were required to provide to PowerSchool.

136. PowerSchool further enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

137. Instead of providing a reasonable level of security that would have prevented the Data Breach, PowerSchool calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members suffered as a direct and proximate result of PowerSchool's failure to provide the requisite security.

138. Because of their abject failure to safeguard the PII, PowerSchool has unjustly received and retained monetary benefits from Plaintiffs and Class Members. Principles of equity and good conscience do not permit PowerSchool to retain the full value the benefit conferred by Plaintiffs and Class Members' PII because PowerSchool failed to adequately protect their PII.

139. Plaintiffs and Class Members are therefore entitled to relief, including disgorgement of all revenues and profits that PowerSchool earned as a result of its unlawful and wrongful conduct.

COUNT IV

Invasion of Privacy

140. Plaintiffs re-allege and incorporate by reference paragraphs 1-105 of the Complaint as if fully set forth herein.

141. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their highly confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

142. PowerSchool owed a duty to its consumers, including Plaintiffs and Class Members, to keep this information confidential.

143. PowerSchool intentionally intruded upon the solitude, seclusion, and private affairs of Plaintiffs and Class Members by intentionally configuring its systems in such a way that left them vulnerable to cyber-attack, which compromised Plaintiffs and Class Members' personal information.

144. PowerSchool's conduct is especially egregious and offensive as it failed to implement adequate security measures to prevent, track, or detect unauthorized access to Plaintiffs' and Class Members' PII in a timely fashion.

145. The disclosure of the sensitive and confidential personal information of thousands of consumers was highly offensive to Plaintiffs and Class Members because it violated expectations of

privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

146. PowerSchool's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. PowerSchool's conduct would be especially egregious to a reasonable person as PowerSchool publicly disclosed Plaintiffs' and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

147. Plaintiffs and Class Members have been damaged as a direct and proximate result of PowerSchool's invasion of their privacy rights and are entitled to just compensation.

148. Unless and until enjoined and restrained by order of this Court, PowerSchool's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by PowerSchool with its inadequate cybersecurity system and policies.

149. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to PowerSchool's continued possession of their sensitive and confidential records. A judgment for monetary damages will not remedy PowerSchool's inability to safeguard the PII of Plaintiffs and the Class.

150. In addition to injunctive relief, Plaintiffs, on behalf of their children and the other Class Members, also seek compensatory damages for PowerSchool's invasion of privacy, which includes the value of the privacy interest invaded by PowerSchool, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V

Violation of the California Unfair Competition Law

Cal. Bus. & Prof. Code §17200 *et seq.*

151. Plaintiffs re-allege and incorporate by reference paragraphs 1-105 of the Complaint as if fully set forth herein.

152. PowerSchool is a "person" defined by Cal. Bus. & Prof. Code § 17201.

153. PowerSchool violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

154. PowerSchool's "unfair" acts and practices include:

a. utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' personal information; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information.

155. PowerSchool engaged in "unlawful" business practices by violating multiple laws, including the FTC Act (15 U.S.C. § 45), the California Consumer Privacy Act (Cal. Civ. Code § 1798.150), the California Customer Records Act (Cal. Civ. Code § 1798.80, *et seq*), and California common law.

156. PowerSchool's unlawful, unfair, and deceptive acts and practices include:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' personal information, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII;

d. misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII; and

f. failing to promptly and adequately advise Plaintiffs and Class Members of the Data Breach.

157. PowerSchool's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PowerSchool's data security and ability to protect the confidentiality of consumers' personal information.

158. As a direct and proximate result of PowerSchool's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and Class Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

159. PowerSchool's violations were, and are, willful, deceptive, unfair, and unconscionable.

160. By deceptively storing, collecting, and disclosing their PII, PowerSchool has taken money or property from Plaintiffs and Class Members.

161. PowerSchool acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and Class Members' rights.

162. Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from PowerSchool's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request the following relief:

A. A determination that this action is a proper class action under Federal Rule of Civil Procedure 23, appointing Plaintiffs as class representatives, and appointing the undersigned counsel as Class counsel;

B. An award of compensatory damages, punitive damages, statutory or civil penalties to Plaintiffs and the Class as warranted by applicable law;

C. Injunctive or other equitable relief that directs PowerSchool to implement reasonable security procedures and practices to protect users' PII that conform to relevant federal and state guidelines and industry norms;

D. Awarding Plaintiffs and the Class reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

E. Such other relief as the Court may deem just and proper.

VIII. JURY DEMAND

Plaintiffs demand trial by jury of all issues so triable as of right.

DATED: February 13, 2025

/s/ Joseph R. Saveri

JOSEPH SAVERI LAW FIRM, LLP
Joseph R. Saveri (SBN 130064)
Cadio Zirpoli (SBN 179108)
Ronnie Seidel Spiegel* (*Pro Hac Vice F*orthcoming)
Christopher K.L. Young (SBN 318371)
Kevin E. Rayhill (SBN 267496)
601 California Street, Suite 1505
San Francisco, CA 94108
Tel (415) 500-6800
jsaveri@saverilawfirm.com
czirpoli@saverilawfirm.com
rspiegel@sverilawfirm.com
cyoung@saverilawfirm.com
krayhill@saverilawfirm.com

* Located in Washington State

KOZYAK TROPIN & THROCKMORTON, LLP
Robert Neary
(Fla. Bar No. 81712, *Pro Hac Vice Forthcoming*)
Benjamin Widlanski
(Fla. Bar No. 1010644, *Pro Hac Vice Forthcoming*)
Gail McQuilkin
(Fla. Bar No. 969338, *Pro Hac Vice Forthcoming*)
Daniel Herrera
(Fla. Bar No. 1048643, *Pro Hac Vice Forthcoming*)
2525 Ponce de Leon Blvd., Floor 9

Coral Gables, FL 33134
Tel (305) 372-1800
rn@kttlaw.com
bwidlanski@kttlaw.com
gam@kttlaw.com
dherrera@kttlaw.com

Attorneys for Plaintiffs