David S. Casey, Jr., Cal. State Bar No. 60768
dcasey@cglaw.com
CASEY GERRY FRANCAVILLA BLATT LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811

Carol C. Villegas, N.Y. State Bar No. 4154324*
cvillegas@labaton.com
LABATON KELLER SUCHAROW LLP
140 Broadway
New York, New York 10005
Tel.: (212) 907-0700

James J. Pizzirusso, D.C. State Bar No. 477604*
jpizzirusso@hausfeld.com
HAUSFELD LLP
1200 17th Street, N.W., Suite 600
Washington, DC 20036
Tel.: (202) 540-7200

Interim Co-Lead Counsel

**Admitted Pro Hac Vice*
[Additional Counsel listed below]

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

IN RE: POWERSCHOOL HOLDINGS, INC. AND POWERSCHOOL GROUP, LLC CUSTOMER SECURITY BREACH LITIGATION,

Case No.: 25-md-3149-BEN-MSB

MDL NO. 3149

CONSOLIDATED MDL DOCKET

CONSOLIDATED INDIVIDUAL USERS CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

I. INTRODUCTION 2
II. PARTIES 10
III. JURISDICTION AND VENUE 13
IV. FACTUAL ALLEGATIONS 14
A. About PowerSchool, An Education Software Company 14
B. PowerSchool Operates Data-Driven Software 15
C. PowerSchool Repeatedly Assured Users That Their Data Would Be Secure 17
D. Bain Capital Established Playbook: Driving Profits Through Aggressive Offshoring and Cost-Cutting 20
E. Bain's Approach and Discussion with PowerSchool 21
F. Bain Signs Merger Agreement with PowerSchool 24
G. Bain Failed to Assess and Mitigate Data-Breach Risks 27
H. Bain Directed Layoffs and Offshore Expansion 29
I. Bain's Control Post-Merger and Its Impact on Cybersecurity and Staffing ... 31
J. After Acquiring PowerSchool, Bain Failed to Implement the Basic Security Measures Necessary to Protect the Information Bain and PowerSchool Had in Their Possession 32
K. PowerSchool Outsources Support to Movate 33
L. Cybercriminals Easily Export Sensitive Records from PowerSchool, Posing an Ongoing Risk to Millions of Teachers and Families 34
M. The Breach Was Foreseeable 45
N. Defendants Failed to Take Necessary or Reasonable Steps to Safeguard PII 55
O. Compromised Data Presents Serious Risk of Identity Theft 71
P. PowerSchool Has Failed to Offer Adequate Remedies to Protect Students and Educators 84
Q. Plaintiffs' Experiences or Injuries 87
V. CLASS ALLEGATIONS 193

COUNT I – NEGLIGENCE 196
COUNT II – NEGLIGENCE PER SE 205
COUNT III – UNJUST ENRICHMENT 210
COUNT IV - INVASION OF PRIVACY 214
COUNT VI – DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF 217
COUNT VII – BREACH OF FIDUCIARY DUTY 222
COUNT IX – NEGLIGENT TRAINING AND SUPERVISION 224
COUNT X – ALABAMA DECEPTIVE TRADE PRACTICES ACT 229
COUNT XI - ARIZONA CONSUMER FRAUD ACT 233
COUNT XII – CALIFORNIA CUSTOMER RECORDS ACT 236
COUNT XIII – VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT 238
COUNT XIV–CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT 241
COUNT XV – INVASION OF PRIVACY 249
COUNT XVI – CALIFORNIA UNFAIR COMPETITION LAW 251
COUNT XVII – AIDING AND ABETTING. 255
COUNT XVIII – CALIFORNIA CONSUMER LEGAL REMEDIES ACT 257
COUNT XIX – CALIFORNIA'S COMPREHENSIVE DATA ACCESS AND FRAUD ACT 260
COUNT XX – CALIFORNIA'S PROHIBITION AGAINST DECEIT BY CONCEALMENT 262
COUNT XXI – COLORADO SECURITY BREACH NOTIFICATION ACT 263
COUNT XXII – COLORADO CONSUMER PROTECTION ACT 264

TABLE OF CONTENTS

COUNT XXIII – FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT 268

COUNT XXIV – GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT 270

COUNT XXV – RECOVERY OF EXPENSES OF LITIGATION 274

COUNT XXVI – IDAHO CONSUMER PROTECTION ACT 274

COUNT XXVII – ILLINOIS PERSONAL INFORMATION PROTECTION ACT 278

COUNT XXVIII – ILLINOIS CONSUMER FRAUD ACT 279

COUNT XXIX – ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT 282

COUNT XXX – INDIANA DECEPTIVE CONSUMER SALES ACT 285

COUNT XXXI – PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW 291

COUNT XXXII – IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT 292

COUNT XXXIII – PROTECTION OF CONSUMER INFORMATION 294

COUNT XXXIV – KANSAS CONSUMER PROTECTION ACT 296

COUNT XXXV – DATABASE SECURITY BREACH NOTIFICATION LAW ..300

COUNT XXXVI – LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW 301

COUNT XXXVII – MAINE UNFAIR TRADE PRACTICES ACT 304

COUNT XXXVIII – MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT 307

COUNT XXXIX – MARYLAND PERSONAL INFORMATION PROTECTION ACT 310

COUNT XL – MARYLAND CONSUMER PROTECTION ACT 312

TABLE OF CONTENTS

COUNT XLI – MASSACHUSETTS CONSUMER PROTECTION ACT 316

COUNT XLII - MICHIGAN IDENTITY THEFT PROTECTION ACT 319

COUNT XLIII - MICHIGAN CONSUMER PROTECTION ACT 320

COUNT XLIV – MINNESOTA CONSUMER FRAUD ACT 323

COUNT XLV – MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT.....326

COUNT XLVI – MISSISSIPPI CONSUMER PROTECTION ACT 329

COUNT XLVII – MISSOURI MERCHANDISING PRACTICES ACT 333

COUNT XLVIII – COMPUTER SECURITY BREACH LAW 335

COUNT XLIX – MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT.....336

COUNT L – NOTICE OF SECURITY BREACH 339

COUNT LI – NEW HAMPSHIRE CONSUMER PROTECTION ACT 340

COUNT LII – NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT.....343

COUNT LIII – NEW JERSEY CONSUMER FRAUD ACT.....344

COUNT LIV – NEW MEXICO UNFAIR PRACTICES ACT 347

COUNT LV – NEW YORK GENERAL BUSINESS LAW.....350

COUNT LVI – NORTH CAROLINA IDENTITY THEFT PROTECTION ACT ..353

COUNT LVII – NORTH CAROLINA UNFAIR TRADE PRACTICES ACT.....354

COUNT LVIII - NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION.....357

COUNT LIX - NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT. 358

COUNT LX – OHIO CONSUMER SALES PRACTICES ACT 361

TABLE OF CONTENTS

COUNT LXI – OHIO DECEPTIVE TRADE PRACTICES ACT 364

COUNT LXII - OKLAHOMA CONSUMER PROTECTION ACT.....367

COUNT LXIII – OREGON CONSUMER IDENTITY THEFT PROTECTION ACT 371

COUNT LXIV – OREGON UNLAWFUL TRADE PRACTICES ACT.....372

COUNT LXV – PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW 376

COUNT LXVI – RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT.....379

COUNT LXVII – SOUTH CAROLINA DATA BREACH SECURITY ACT 382

COUNT LXVIII – SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT ...383

COUNT LXIX - TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT 388

COUNT LXX - TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT 389

COUNT LXXI – DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT.....394

COUNT LXXII – UTAH CONSUMER SALES PRACTICES ACT 399

COUNT LXXIII – VERMONT CONSUMER FRAUD ACT.....404

COUNT LXXIV – VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT 408

COUNT LXXV – VIRGINIA CONSUMER PROTECTION ACT.....409

COUNT LXXVI - WASHINGTON DATA BREACH NOTICE ACT 413

COUNT LXXVII – WASHINGTON CONSUMER PROTECTION ACT 414

COUNT LXXVIII – NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION.....417

COUNT LXXIX – WISCONSIN DECEPTIVE TRADE PRACTICES ACT.....418

COUNT LXXX – COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS 422

COUNT LXXXI – WYOMING CONSUMER PROTECTION ACT 423

PRAYER FOR RELIEF 427

JURY TRIAL DEMAND 428

TABLE OF CONTENTS

Plaintiffs, individually and on the below-defined Classes or Subclasses (collectively "Plaintiffs"), by and through their undersigned attorneys, bring this Consolidated Amended Class Action Complaint on behalf of themselves and all others similarly situated (the "Class Members"), against Defendants PowerSchool Holdings, Inc. and PowerSchool Group, LLC (together, "PowerSchool" or "the Company"), Bain Capital, LP ("Bain Capital" or "Bain"), and Movate, Inc. ("Movate") (PowerSchool, Bain, and Movate, referred to herein as "Defendants" unless otherwise specified) and allege, upon personal information and belief and the investigation of their counsel, including consultation with experts, that PowerSchool failed to safeguard highly sensitive personally identifiable information ("PII") and personal health information ("PHI") of students, teachers, and other individuals, including minors, using PowerSchool software products, including their names, social security numbers ("SSN"), demographic information, dates of birth, phone numbers, email addresses, and medical information, and were damaged thereby (collectively this data is referred to as "PII"). Plaintiffs pursue claims on behalf of the Classes or Subclasses under California law in accordance with Defendants' terms of service.

Plaintiffs and Class Members entrusted Defendant PowerSchool with their highly sensitive PII and reasonably expected that PowerSchool would safeguard their data at least in accordance with PowerSchool's representations. PowerSchool knew the sensitive PII it maintained is the type of information highly sought after by hackers. With this knowledge, PowerSchool assured its customers that all user data PowerSchool retained or collected would be kept safe. For this reason, PowerSchool knew or should have known that it needed to employ reasonable measures to protect Plaintiffs' and Class Members' highly sensitive PII from unauthorized disclosure but nevertheless permitted a serious system vulnerability to arise and be exploited, resulting in the massive Data Breach in December 2024. After exposing tens of millions

of students' and teachers' PII, PowerSchool then further exacerbated the problem and failed to timely and properly notify Plaintiff and Class Members. To date, PowerSchool has still failed to adequately provide notice of the Data Breach to affected individuals. As a result of PowerSchool's misconduct, Plaintiffs and Class Members have suffered and will continue to suffer harm and damages.

The information pled herein is based on the information currently available publicly and as a result of diligent investigation. Plaintiffs anticipate that additional information will be made available as future updates are disseminated and in discovery. This forthcoming information is likely to add to the claims herein, including Plaintiffs' claims of ongoing harm.

I. INTRODUCTION[1]

1. This class action stems from the December 2024 data breach of Defendant PowerSchool's Student Information System ("SIS")—seemingly the largest data breach in history involving the educational sector—caused by Defendants' failure to safeguard the sensitive PII of over ***70 million*** schoolchildren, their families, and teachers (the "Data Breach").

2. The stolen PII consists of the most private information an individual holds dear, including their name, SSN, birthdate, demographic information, phone number, email address, medical information, academic performance such as grades and attendance records, child custody status, reduced meal status, banking and financial information, student and staff identification number, and Individualized Education Program ("IEP") details such as specific accommodations for students with special needs.

3. Headquartered in Folsom, California, PowerSchool provides educational software services to an estimated 18,000 customers worldwide, which include the

[1] All emphasis throughout is added unless otherwise noted.

country's largest schools and school districts; PowerSchool's services cover a variety of administrative tasks ranging from enrollment to curriculum and teacher recruitment.

4. PowerSchool's main product offering is through various platforms called SIS, which PowerSchool touts as: "one ***secure*** customizable platform providing the interoperability need to power your school and district operations with accurate student data."[2] Notably, SIS does not only gather student data; it facilitates "gather[ing] ***vital information*** from families and staff."[3]

5. In other words, PowerSchool's business revolves around, and depends upon, receiving and maintaining sensitive PII from schoolchildren, their families, and schoolteachers. Indeed, as a result of a minor's enrollment as a student or by a condition of employment as a teacher, tens of millions of individuals are required to input or have their PII input into SIS simply because a student and/or teacher's school utilizes PowerSchool's SIS.

6. Companies entrusted with this type of sensitive information are required—by state and federal law—to take steps to protect it. To this end, PowerSchool repeatedly represented through its privacy policies, practices, and postings on its website that it actively took steps to protect the PII in its care. PowerSchool's website confirmed that "the safe collection and management of student data is essential"[4] and that "PowerSchool is committed to being a good custodian of student data – taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[5]

7. As such, PowerSchool understood the highly sensitive nature of the PII it was gathering and maintaining. Through these representations, Defendants promised

---

[2] *PowerSchool SIS at-a-glance*, PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/#video (last visited Jan. 17, 2025).

[3] *Id.*

[4] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

[5] *Id.*

that they would take meaningful steps to safeguard their users' PII, consistent with Defendants' duty to maintain the security of Plaintiffs' and Class members' PII.

8. PowerSchool inadequately maintained its network security, its platform, and its software, however, making SIS—a PII treasure trove—an easy target. PowerSchool knew, or should have known, that it had not come close to implementing minimum cybersecurity protections for SIS, and that the absence of basic data security practices vastly increased the risk of a data breach occurring.

9. PowerSchool, among other things, (1) failed to require a multi-factor authentication procedure to enter its systems; (2) failed to require users to change their passwords; and (3) permitted individuals to access PII despite those individuals not needing access to that PII to do their jobs. PowerSchool also failed to encrypt PII within its systems. Had PowerSchool taken just ***one*** of these basic security measures, the Data Breach could have been easily averted.

10. The Data Breach unfolded over several months; the threat actor(s) first breached PowerSchool's systems using compromised credentials as early as September 4, 2024.[6] Yet, their access went undetected. When the threat actor(s) returned on December 20, 2024, access again went undetected as 70 million students, teachers, and their families' PII was quickly exfiltrated.[7]

11. Making matters worse, PowerSchool rewarded the threat actor(s) by fulfilling their ransom request in exchange for the purported deletion of the stolen data.[8] Unsurprisingly, however, the threat actor(s) did not honor their side of the bargain, as evidenced by extortion email attacks acknowledged by certain schools in the United

[6] *United States v. Lane*, No. 25-cr-40015, ECF No. 1 (D. Mass. May 20, 2025) (the "Charging Document").

[7] *Id.*

[8] Kevin Collier, *School districts hit with extortion attempts months after education tech data breach*, NBC News (May 7, 2025), https://www.nbcnews.com/tech/security/school-districts-hit-extortion-attempts-powerschool-breach-rcna205429 (last visited July 31, 2025).

States and Canada, occurring as recently as early May 2025—using the same data "previously stolen in December" that was purportedly deleted.[9]

12. After permitting the exfiltration of massive troves of PII, PowerSchool made the situation worse and failed to timely and properly notify affected individuals of the Data Breach; indeed, it took until January 7, 2025 for PowerSchool to even publicly acknowledge the Data Breach—almost three full weeks after the data was stolen. Additionally, it remains unclear how much PowerSchool paid for ransom. The threat actor(s) demanded 30 Bitcoin (about $2.85 million at that time); PowerSchool has failed to disclose the amount it actually paid.

13. PowerSchool, which develops software programs to help schools manage students, data and educational programming, grew exponentially in recent years, especially during the Covid pandemic, when many schools shifted to remote learning.

14. But PowerSchool's problems started well before the breach and were exacerbated by private equity behemoth and co-Defendant Bain Capital's merger with PowerSchool. In August 2022, Defendant Bain Capital approached PowerSchool about a potential business combination.[10] Talks unfolded over the ensuing two years, culminating in Defendants Bain Capital and PowerSchool signing a Merger Agreement in June 2024 (the "Merger Agreement")—approximately just three months before PowerSchool's systems were first breached.[11]

15. With PowerSchool, Bain Capital followed the private equity playbook. By August 2024—just one month before the threat actor(s) made the initial breach—Bain Capital "gutted" 5% of PowerSchool's employees.[12] The mass layoffs, which included

---

[9] Id.

[10] PowerSchool Holdings, Inc., Schedule 14C Information Statement relating to Merger or Acquisition at 21 (Sept. 4, 2024), available at https://www.sec.gov/Archives/edgar/data/1835681/000119312524212624/d836904ddefm14c.htm.

[11] *Id.*

[12] Wyatt Gaylor (@wyattg), X (Aug. 13, 2024, 2:09 PM EST), https://x.com/wyattg/status/1823421671799447980; *see also* PowerTool

Footnote continued on next page

certain longtime employees, were allegedly due to PowerSchool missing its quarterly earnings per share consensus estimate by just one cent.[13]

16. But Bain Capital's plans for PowerSchool were in place well before the consummation of the merger, as seen through Bain's acquisition of Outsourcing, Inc.[14] and the language featured in the Merger Agreement heralding the financial benefits achievable through offshoring PowerSchool's responsibilities. Indeed, in forecasting financial metrics such as adjusted gross profit margins, adjusted research and development costs, and adjusted EBITDA margins, the Merger Agreement repeatedly referenced "***increased use of PowerSchool's offshore centers*** of excellence."[15]

17. After Bain implemented the firing of several long-time employees to support PowerSchool's "increased use" of these purported "offshore centers of excellence;" a vocal few raised their concerns online, writing that a "[l]arge scale layoff" was occurring and that it "is a general trend to outsource all the jobs to offshore…now it's shifting to support and product management."[16] Others mentioned

---

(@PowerTool_), X (Aug. 14, 2024, 2:49 AM EST), https://x.com/PowerTool_/status/1823612984624664959; *see also* PowerTool (@PowerTool_), X (Aug. 17, 2024, 11:51 AM EST), https://x.com/PowerTool_/status/1824836415164735656 (comment from Dominic Butler, Advanced Support Engineer II at PowerSchool, "[PowerSchool] just laid off 5% of their workforce yesterday.").

[13] *Id.*; *PowerSchool Announces Second Quarter Financial Results*, Business Wire (Aug. 9, 2024), available at https://www.businesswire.com/news/home/20240808373822/en/PowerSchool-Announces-Second-Quarter-Financial-Results.

[14] With a hint of foreshadowing, and during negotiations with PowerSchool, Bain Capital announced its acquisition of Outsourcing, Inc. on December 8, 2023. Bain Capital touted that acquisition as one where Bain Capital "hopes to support management in enhancing Outsourcing's competitiveness" with the "goal" of "spread[ing]…remote work…and pursu[ing] higher profit margins" through reducing a company's costs by offshoring work. *See* Statement from Bain Capital Private Equity regarding Outsourcing Inc., Bain Capital (Dec. 8, 2023), https://www.baincapital.com/news/statement-bain-capital-private-equity-regarding-outsourcing-inc (last visited July 1, 2025).

[15] *Supra* note 10 at 84.

[16] Anonymous, Employee Review: PowerSchool Group, Glassdoor (Aug. 19, 2024) , https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW90216913.htm (last visited July 1, 2025).

that PowerSchool was "clearly shifting to an India-based workforce at the expense of US-based employees."[17]

18. Perhaps encapsulating PowerSchool's conversion to private equity most succinctly, one former employee wrote that PowerSchool had "started as a mission-driven company to help every student achieve quickly became a profit-first march towards ed-tech domination."[18]

19. In other words, Bain Capital moved to reduce costs and maximize profits by culling PowerSchool's U.S. workforce and replacing them with discounted international labor—all at the expense of cybersecurity, data protection, and ultimately, 70 million students, their families, and teachers.

20. Offshoring work often takes the form of one company hiring another to subcontract out the hiring company's responsibilities. Here, PowerSchool tapped co-Defendant Movate for subcontractor services involving technical support and network operations as early as July 2024.[19]

21. The Data Breach was facilitated by the misappropriation and use of an authorized individual's credentials (username and password). Upon information and belief, the credentials the threat actors exploited to gain access to SIS were Rayson Cruz's. Per Cruz's LinkedIn page, he has worked for Movate since February 2019.[20]

---

[17] Anonymous, Employee Review of PowerSchool Group (Aug. 20, 2024) (Glassdoor.com), https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW90258225.htm (last visited July 1, 2025).

[18] Anonymous, Employee Review of PowerSchool Group (Sep. 12, 2024) (Glassdoor.com), https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW90973925.htm (last visited July 1, 2025).

[19] MOVATE PHILIPPINES INC., "MOVATE PHILIPPINES INC. is now hiring for TECHICAL SUPPORT agents…" (Facebook Group: Movate Philippines Inc.), July 24, 2024, https://www.facebook.com/groups/1175349822483308/posts/8616442245040658ph.jobstreet.com+1m.faceb.

[20] Rayson Cruz, LinkedIn Profile (accessed July 1, 2025), https://www.linkedin.com/in/rayson-cruz-3425bb292/.

22. Various school districts indicated that a "Remote Support connection from the IP address of 91[.]218[.]50[.]11 with the user 'Rayson Cruz' is one of the primary indicators of compromise." [21]

23. PowerSchool provided Movate employees (without multifactor authentication protection) unfettered access to SIS and U.S. students', their families', and teachers' sensitive PII, notwithstanding the absence of other basic cybersecurity measures.

24. Plaintiffs and Class Members' PII were compromised because of Defendants' negligent and/or careless acts and omissions and Defendants' failure to reasonably and adequately protect Plaintiffs' and Class members' PII.

25. In July 2025, Matthew D. Lane, a 19-year-old college student, pleaded guilty to federal charges that he led the massive cyberattack against PowerSchool.

26. Despite his acceptance of a guilty plea, an unknown number of threat actors, cybercriminals, hackers, can use the PII accessed in the Data Breach to harm Plaintiffs and Class Members indefinitely by targeting them with phishing and hacking attacks, using PII to obtain governmental benefits, filing fraudulent tax forms, extortion, and opening new or compromising current financial accounts.

27. As a result of the Data Breach, in addition to actual harm, such as fraud and identity theft, Plaintiffs and Class Members face a clear and present risk of imminent and certainly impending harm, especially magnified in this instance due to the presence of SSNs and other financial data. Plaintiffs and Class Members have and will continue to suffer injuries stemming from this risk, including, but not limited to, a loss of their valuable data, time and opportunity costs, and mitigation expenses over the misuse of their PII.

[21] *PowerSchool Incident FAQs*, Edutech, https://www.edutech.nd.gov/services/powerschool/powerschool-incident-faqs (last visited Aug. 9, 2025).

28. This risk is rendered more serious because of the amount of time that has passed between the Data Breach and the lack of sufficient notice about the Data Breach.

29. PowerSchool failed to provide timely notice of the Data Breach to Plaintiffs and Class Members, only beginning to provide limited notice in the months after the breach. Indeed, PowerSchool failed to even notify the impacted **schools** until at least January 7, 2025, and, in most cases, January 9, 2025—almost two (2) weeks after PowerSchool learned of the Data Breach.

30. In addition to untimely notice, PowerSchool has also failed to provide sufficient notice of the Data Breach. Specifically, PowerSchool has failed and continues to fail to provide information necessary to assess the full impact of the breach including who or which unauthorized third parties gained access its systems, exactly how long the breach lasted, precisely what data was accessed, viewed, downloaded, and stolen.

31. Even those Class Members who have yet to experience identity theft have had to spend valuable time responding to the Data Breach and have an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Indeed, Plaintiffs and Class Members who received notice of the Data Breach were expressly advised to take action to protect themselves. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of PII and PHI, loss of privacy, benefit of the bargain, nominal damages, and/or additional damages as described below.

32. The unfortunate reality is that this could have been avoided, had Defendants taken adequate and reasonable measures to ensure PowerSchool's data systems were protected against unauthorized intrusions. Instead, each entity neglected industry standards, failed to take standard and reasonably available steps to prevent the

Data Breach, including implementing multi-factor authentication, properly training staff and employees on proper security measures, encrypting PII, all while promising teachers, students, and their parents, premium security measures to maintain an advantage in a highly sensitive and competitive industry. Had Defendants properly monitored PowerSchool's computer network and systems that housed the PII, they would have discovered the intrusion sooner or prevented it altogether.

II. PARTIES

33. Plaintiffs include employees, students, former students, and parents of students at school districts and institutions which used PowerSchool's SIS. Plaintiffs are introduced in Section IV.Q

34. Plaintiff the Providence Teacher's Union ("PTU") is a professional organization asserting claims on behalf of itself and its impacted members. PTU has over 2000 members; members include all regularly appointed teachers, long-term substitutes, and long-term substitutes in pool in Providence, Rhode Island. PTU members used PowerSchool products and software for education services in the course of their employment. As a result, PTU members provided highly sensitive PII to PowerSchool. As a result of PowerSchool's misconduct, which caused the Data Breach, PTU members have had to, and will have to, take measures that would not otherwise be necessary to protect against identity theft and/or credit disruptions. Moreover, PTU has had to expend resources to address members' concerns and experiences as a result of the breach, including answering member calls and questions regarding the breach, the impact of the breach on their employment and potential need to continue using the PowerSchool software.

35. Defendant PowerSchool Group, LLC is a Delaware limited liability company headquartered at 150 Parkshore Drive, Folsom, California 95630.

36. Defendant PowerSchool Holdings, Inc. is a Delaware corporation headquartered at 150 Parkshore Drive, Folsom, California 95630.

37. Defendant Bain Capital, LP is a Delaware limited liability company headquartered at 200 Clarendon St., Boston, Massachusetts 02116. Bain, through its agents/alter egos, fully acquired PowerSchool on or around October 1, 2024, prior to the Data Breach in December 2024.

38. Throughout the events at issue, Defendants PowerSchool Group, LLC, PowerSchool Holdings, Inc. and Bain Capital, LP have operated as one entity with fully coordinated and shared operations. Resources are cross-applied and management decisions for PowerSchool are made by and through the management of Bain. The directors and officers of Bain were and are directly involved in the events at issue in this litigation, including PowerSchool's cybersecurity procedures (or lack thereof), PowerSchool's employees, the Data Breach itself, and PowerSchool's response to the Data Breach. Despite being its parent company, and in a position to do so, Bain not only failed to direct PowerSchool to ensure its cybersecurity was up-to-date, but also engaged in conduct that undermined that cybersecurity. Based upon information and belief, and at least by the October 2024 merger, PowerSchool was controlled by Bain, which influenced and controlled the security standards PowerSchool adopted and represented that it made.

39. To remain separate and distinct for the purposes of liability in this action, Defendants PowerSchool and Bain must operate as separate and distinct legal and operational entities. Here, for the matters and functions alleged and relevant to the Data Breach, PowerSchool Holdings, Inc., PowerSchool Group, LLC, and Bain Capital LP were merely alter egos. For purposes of how student and teacher data was handled, warehoused, used, and sold, the corporate distinctions were disregarded in practice. Defendants shared unity of interest and ownership such that separate personalities of the corporation and subsidiary no longer existed. Further, recognition of the technical corporate formalities in this case would cause irremediable injustice and permit Bain –

the entity whose directors and officers were at the PowerSchool helm during the events alleged herein – to defeat justice and evade responsibility.

40. Alternatively, based on the facts alleged herein and in accord with theories of agency, Bain is liable for the acts of PowerSchool because: (a) it was PowerSchool's parent; and (b) had dominant control over and was involved in PowerSchool's misconduct. As alleged, PowerSchool's misconduct can be traced to Bain, its parent, through post-merger initiatives and the conduct of overlapping officers and directors who were directly responsible for PowerSchool's activities, including its cybersecurity protections or lack thereof. Bain dominates and controls PowerSchool's internal affairs and daily operations. With respect to the breached data of PowerSchool's customers and individual users, the responses to the data breach, and the conduct giving rise to this litigation, Bain had the right to control PowerSchool, and PowerSchool acted as Bain's agent, and was authorized and acted within the scope of authority as dictated by Bain. PowerSchool's activities – which included collecting, obtaining, storing, maintaining, sharing, and making available the sensitive PII and PHI of Plaintiffs and Class Members – resulted in PowerSchool violating the privacy rights of millions of vulnerable students, along with their families, guardians, caregivers, teachers and staff throughout the United States. At all times, the injuries caused by PowerSchool's actions and inactions were foreseeable.

41. Accordingly, for all purposes hereafter and except where otherwise specified, when Plaintiffs allege "PowerSchool" as the actor or responsible party, they are alleging the participation of all three Defendants, PowerSchool Holdings, Inc., PowerSchool Group, LLC, and Bain Capital, LP, collectively.

42. Defendant Movate, Inc. is a Delaware corporation headquartered at 600 Tennyson Parkway, Suite 255, Plano, Texas 75024.

43. Upon information and belief, Movate failed to ensure that its employees, including Rayson Cruz, had adequate protections in place to prevent unauthorized access to PowerSchool's systems including SIS.

III. JURISDICTION AND VENUE

44. This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000 and there are more than 100 proposed Class Members. Minimal diversity exists, as Defendants are citizens of States different from that of at least one Class Member. This Court also has supplemental jurisdiction under 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

45. This Court has personal jurisdiction over PowerSchool because it is headquartered and regularly conducts business in the state of California.

46. This Court has personal jurisdiction over Bain Capital because this action arises from Bain's continuous and systematic contacts with California. Bain Capital maintains control over PowerSchool and assumed the risk of litigation in California when Bain acquired PowerSchool, headquartered in California. Bain was, and is, responsible for many of the critical decisions that gave rise to this action.

47. This Court has personal jurisdiction over Movate because this action arises from Movate's continuous and systematic contacts with California. Movate Defendants exercised control over Plaintiffs' data and directed contacts to California through technical support for PowerSchool customers, including California school districts.

48. Venue is proper in this District under 28 U.S.C. §1407, Rule 7.1 of the Rules of Procedure of the JPML, and the Transfer Order related to this matter and any future Transfer Orders as the JPML may issue. In the alternative, venue is proper in

this District pursuant to 28 U.S.C. § 1391, because PowerSchool's principal place of business is in the state of California.

IV. FACTUAL ALLEGATIONS

A. ABOUT POWERSCHOOL, AN EDUCATION SOFTWARE COMPANY

49. Created in 1983, PowerSchool was designed as a record-keeping software for student attendance and educational information.[22]

50. Today, particularly as a result of the Covid Pandemic and remote learning, PowerSchool has grown to be the leading provider of cloud-based software for K-12 education in the United States, supplying schools and school districts with a "broad range of mission-critical capabilities," such as the core system of record used by districts and schools, student and teacher assessment tools, learning management systems, teacher hiring and retention solutions, and analytics powered by artificial intelligence ("AI").[23]

51. PowerSchool sells its software to schools and school districts nationwide, including over 90 of the 100 largest U.S. school districts by student enrollment; in North America, PowerSchool is an education hegemon—in the U.S. and Canada alone, ***over 80% of all K-12 students*** use PowerSchool products.[24] PowerSchool also operates in more than 95 countries globally.[25]

52. PowerSchool's software is made available to end users, like students, parents, and teachers, all of whom rely on the software daily to facilitate educational

---

[22] Scott Lillis, Greg Porter, *Founder of PowerSchool, Founders Parade* (June 1, 2019), https://blogs.ubc.ca/etec522/2022/09/28/greg-porter-founder-of-powerschool-by-scott-lillis/ (last visited July 3, 2025).

[23] PowerSchool Holdings, Inc., Annual Report (Form 10-K), (March 1, 2024) https://www.sec.gov/ix?doc=/Archives/edgar/data/0001835681/000183568124000016/pwsc-20231231.htm.

[24] *Id.*

[25] *Id.*

and administrative functions. PowerSchool offers a variety of cloud-software products to schools for these purposes.

53. One of PowerSchool's leading products is the PowerSchool SIS, used by at least 15,000 schools and districts.[26] PowerSchool markets SIS as a solution to "save time, reduce costs, improve student outcomes, and increase security"[27] and further represents that SIS is "for students" and can "increase family engagement, improve student accountability, and provide peace of mind with a secure, configurable system . . . for compliance reporting, classroom management, and family communication."[28]

B. POWERSCHOOL OPERATES DATA-DRIVEN SOFTWARE

54. PowerSchool's leading SIS software product is designed to enable schools and school districts to collect and manage large swaths of information related to students and teachers, including highly sensitive PII and student records.

55. PowerSchool SIS offers school districts various software tools that allows schools to offer portals to students and parents to access educational information including grades, student schedules, announcements, and attendance.

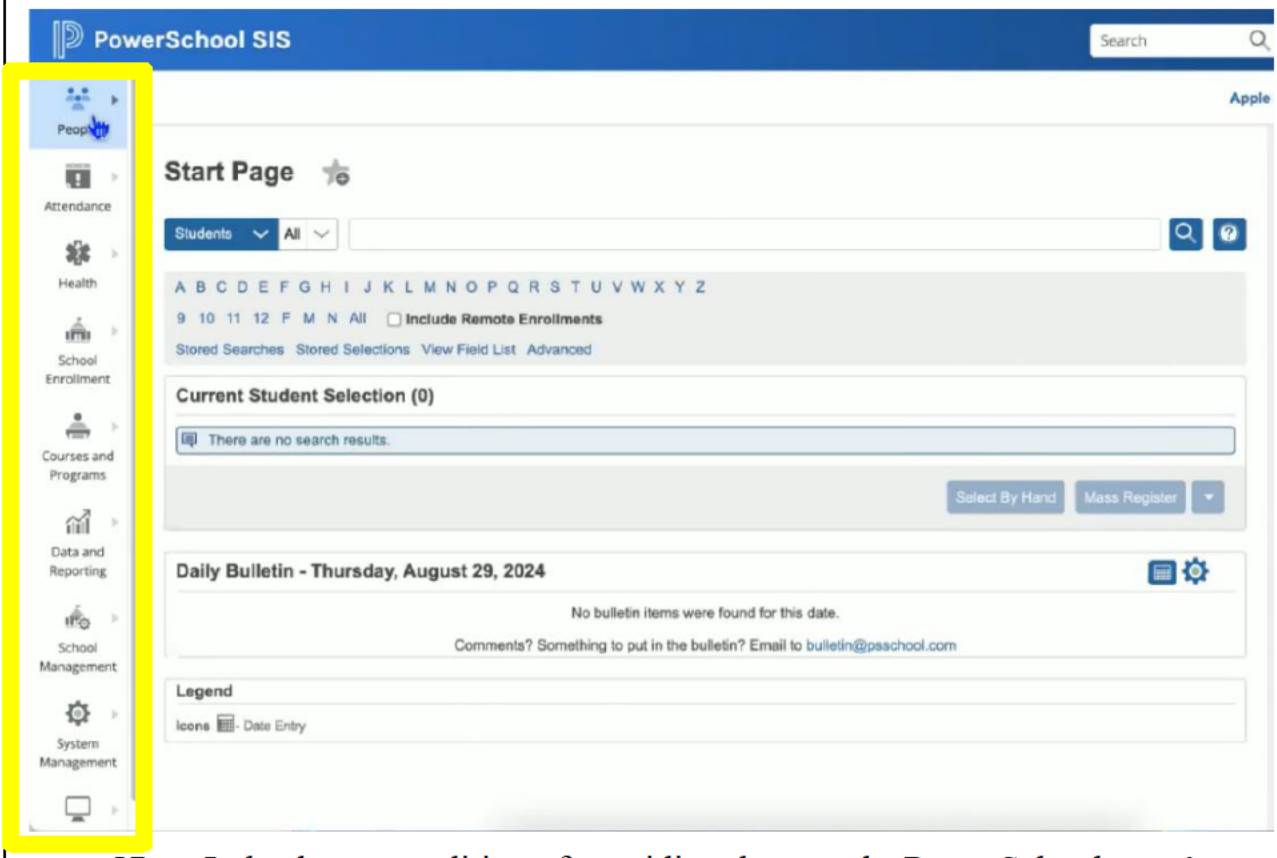
56. PowerSchool's SIS product also serves as a repository for the highly sensitive data schools and school districts must collect about students and teachers for education and employment services, respectively. This information includes attendance, grades, behavior, SSNs, demography, graduation tracking, and health related information, such as IEPs. Figure [[1]] demonstrates PowerSchool's capabilities.

Figure [[1]]

[26] *40,000 Students Start School on Time Because of 90-Day PowerSchool SIS Implementation*, PowerSchool, https://www.powerschool.com/case-studies/40000-students-start-school-on-time-because-of-90-day-powerschool-sis-implementation/ (last visited May 13, 2025).

[27] *Solutions*, POWERSCHOOL GROUP, LLC, https://www.powerschool.com/solutions/ (last visited July 3, 2025).

[28] *Id.*



57. Indeed, as a condition of providing these tools, PowerSchool ***requires*** end users, like students and teachers, to input highly sensitive PII, including:

(a) Name

(b) Email Address

(c) Social Security Number

(d) Address

(e) Phone Number

(f) Emergency Contact Information

(g) Birth Date

(h) Demographic Profile

(i) Ethnicity

(j) Grades

(k) Gender

(l) Device Information (*e.g.* unique device ID, IP address, and cookies)

(m) Class Schedule

(n) Standardized Test Scores

(o) Allergy Information

(p) Immunization Records

(q) Learning Disabilities/Special Education Status

(r) Other medical-related information

(s) Lunch Balances/Reduced Price Meal Status

(t) Attendance

(u) Disciplinary Notes/Records

(v) Child Custody Information, including child custody agreements, parent restraining orders, and other legal information

(w) Credit and/or debit card information (*i.e.* first and last name, card number, expiration date, card verification value (CVV), and zip code, as required)

58. With over 15,000 schools and school districts using PowerSchool SIS, potentially tens of millions of teachers', students', and parents' PII were input and entrusted to PowerSchool.

C. POWERSCHOOL REPEATEDLY ASSURED USERS THAT THEIR DATA WOULD BE SECURE

59. PowerSchool understood the sensitive nature of the PII teachers, students, and parents entrusted in the SIS system. Indeed, PowerSchool explicitly recognized the risk of unauthorized data access or disclosure, stating on its website: "PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. ***We strive to continuously maintain reasonable physical, administrative, and technical security measures.***"[29]

[29] *Privacy,* PowerSchool (last updated Feb. 2, 2023) https://www.powerschool.com/legal/privacy-2023/.

60. Because of these known risks, PowerSchool assured users that their PII would be protected. For example, on its website, PowerSchool confirmed that "the safe collection and management of student data is essential"[30] and that "PowerSchool is committed to being a good custodian of student data – taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[31]

61. To that end, PowerSchool represented that it would "protect[] students' data with a comprehensive security program that starts with 'secure by design' principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center" and even stated that its "products are independently validated by third-party auditors."

How PowerSchool Protects Data

We are dedicated to protecting your students' data with a comprehensive security program that starts with "secure by design" principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool. To learn more visit our security page.

62. In addition to publicly touting its data security practices, PowerSchool took a pledge to maintain student privacy by signing the National Student Privacy Pledge, a voluntary, public, and legally enforceable statement by edtech companies to safeguard student privacy.[32]

[30] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited Jan. 17, 2025).

[31] *Student Data Privacy: Everything you Need to Know*, PowerSchool (June 20, 2023) https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/..

[32] *Student Privacy Pledge: About The Pledge*, Student Privacy Pledge https://studentprivacypledge.org/.

Figure [[2]]

63. As depicted in Figure [[2]], PowerSchool assured educators and schools that they could have "peace of mind" and provide assurances that "student data is safe."[33]

64. In keeping with these assurances, PowerSchool also issued a quarterly Information Security Report "meant to provide [its] customers with additional transparency about cybersecurity at PowerSchool."[34]

65. Additionally, PowerSchool represented that it complied with applicable regulations, including FERPA, the General Data Protection Regulation (GDPR), the Children's Online Privacy Protection Act (COPPA), and other state and federal regulations.[35]

[33] As of April 25, 2025, the Student Privacy Pledge announced its retirement. However, "participating companies remain legally bound by Pledge commitments with regard to data collected during the period they were signatories." *See id.*
[34] *See supra* note 30.
[35] *See id.*

D. BAIN CAPITAL ESTABLISHED PLAYBOOK: DRIVING PROFITS THROUGH AGGRESSIVE OFFSHORING AND COST-CUTTING

66. Bain Capital is a multi-national private multi-asset alternative investment firm that operates across various asset classes, including private equity, credit, public equity, venture capital, and others. Bain's profit model depends heavily on leveraged buyouts under which it purchases public companies, takes them private, and then works to improve the company's balance sheet with the purpose of later selling it, while taking dividends from the purchased company to pay its investors. Operational changes made by Bain typically include an emphasis on cost reduction including the outsourcing of key functions to cheaper and less regulated overseas markets.

67. From the early 1990s onward, Bain developed a clear and consistent strategy: acquire or invest in companies, then rapidly expand their offshore operations to cut costs, often at the expense of U.S. jobs and to avoid U.S. regulations.

68. This started in 1993, when Bain entered the outsourcing business through its investment in CSI, which initially provided a variety of services to technological companies like Microsoft, including customer support. Within just a few years, CSI was soon rebranded as Stream International, aggressively establishing call centers in Europe, Asia, under Bain's direction. Bain, at the time while still a minority shareholder, was an active investor and steered the company into offshore support. By 1999 Bain became the majority shareholder, cementing Stream as a major offshore player.[36] The same strategy applied across other investments - Modus Media, SMTC Corp., Sensata Technologies, and more[37] – where Bain's acquisition or investment

[36] *Romney's Bain Capital invested in companies that moved jobs overseas*, THE WASHINGTON POST (June 2012), https://www.washingtonpost.com/business/economy/romneys-bain-capital-invested-in-companies-that-moved-jobs-overseas/2012/06/21/gJQAsD9ptV_story.html.

[37] Josh Eidelson, *Bain offshoring victims ask Romney for help*, SALON (July 2012), https://www.salon.com/2012/07/17/bain_off_shoring_victims_ask_romney_for_help/.

likewise targeted offshoring labor and production, to lower costs. The most telling is Sensata Technologies: when Bain acquired it in 2006, Sensata's U.S. workforce was 17%, and within a few years under Bain's ownership, it dropped below 10% - around 170 U.S. jobs were eliminated.

69. Across multiple industries—from manufacturing to technology—Bain's portfolio companies have downsized domestic operations and expanded internationally to maximize profits, often shortly after acquisition. As demonstrated through its prior actions, Bain has a consistent playbook: U.S. facilities are shuttered, domestic workers are displaced, and operations are moved overseas under Bain's direction and control to cut costs and increase profits.

70. Bain's focus on cutting costs and increasing profits comes at the expense of other services, like cybersecurity.

E. BAIN'S APPROACH AND DISCUSSION WITH POWERSCHOOL

71. Beginning on August 31, 2022, and in the midst of the Pandemic while PowerSchool was booming, representatives of Bain Capital approached PowerSchool, through PowerSchool's co-chairperson of the board who was also the representative of Onex, a significant shareholder of PowerSchool, to express interest in discussing a potential business combination or acquisition.[38]

72. For more than two years, Bain maintained an active dialogue with PowerSchool's CEO, Hardeep Gulati, and with the company's principal shareholders, repeatedly discussing PowerSchool's "organic growth potential and strategic [merger & acquisition] opportunities."[39]

73. Consistent with these strategic discussions, on January 8, 2024, PowerSchool announced that it would expand its outsourcing to India from 1,300

[38] PowerSchool Holdings, Inc., Schedule 14C Information (Form PRELI M-14C) (July 23, 2024), https://www.sec.gov/Archives/edgar/data/1835681/000119312524182995/d836904dprem14c.htm .

[39] *Id*.

employees to 2,000, within 3-5 years. The timing and scale of the announcement matched Bain's typical investment playbook, signally that Bain's strategic priorities were already shaping corporate decisions even before the merger was formally signed.[40]

74. Bain worked closely with PowerSchool's leadership to ensure that its future plans aligned with Bain's, including the outsourcing of cybersecurity and IT functions prior to actually taking complete ownership of PowerSchool. As part of any LBO transaction, Bain, the prospective purchaser, would want to ensure that its valuation of the proposed acquisition, PowerSchool, remained consistent during the period of negotiation and into the actual purchase of the company.[41]

75. A few months later, on March 27, 2024, just before the deal was finalized, PowerSchool's Chief Financial Officer ("CFO") Eric Shander presented a set of long-range management forecasts to the board, projecting through 2034, which included ambitious projections of total revenue, adjusted EBITDA,[42] free cash flow, and unlevered cash flow. These forecasts were provided to Bain as part of the continued discussions leading to the signed Merger Agreement and demonstrate Bain's ongoing influence with PowerSchool prior to formal consummation.

76. The forecasts indicated a heavy reliance on offshoring positions to reduce company costs and increase profits, as they showed EBITDA margins increasing significantly from around 35.2% in 2024 to around 47.5% in 2034. The improved EBITDA margin reflected PowerSchool and Bain's expectation that PowerSchool

[40] *PowerSchool Announces Strategic Expansion in India*, POWERSCHOOL, https://www.powerschool.com/news/powerschool-announces-strategic-expansion-in-india/ (last accessed July 21, 2025).

[41] *Leveraged Buyout Process*, CARTA, https://carta.com/learn/startups/exit-strategies/mergers-acquisitions/leveraged-buyout/#identifying-a-target-company (last accessed July 29, 2025).

[42] Earnings Before Interest, Taxes, Depreciation, and Amortization.

would become more efficient in its operations, driven in part by its "increased utilization of offshore centers of excellence."[43]

77. With revenue projected to grow from $788 million in 2024 to $2.76 billion in 2034, PowerSchool demonstrated the potential to expand its market presence.[44] This upward trajectory was an opportunity to use cost-cutting measures like offshoring—a common tactic Bain implemented as part of its leveraged buyouts.

78. As revenue increases, the need to scale operations also increases. By offshoring lower-cost labor, particularly in IT, cybersecurity, and customer support roles, Bain could assist PowerSchool in increasing its profitability without also increasing its operational costs significantly. This would improve margins and contribute to the projected increase in Adjusted EBITDA, which was expected to grow from $277 million in 2024 to $986 million in 2034.

79. PowerSchool's projected increase in revenue and EBITDA margins, driven by cost-cutting measures in consultation with Bain came at the expense of PowerSchool's internal security capabilities as higher-cost (and more highly experienced) U.S.-based engineering, IT, and security staff were replaced with lower-cost overseas labor, typically outsourced through intermediaries rather than directly employed by PowerSchool.

80. Bain Capital ultimately adopted these forecasts, relying on them when negotiating both price and debt structure. Thus, well before closing, Bain ratified and conditioned its offer on cost-reduction measures consistent with its acquisition strategy: removing experienced U.S. labor while expanding inexperienced and low-cost offshore hiring, typically through third-party outsourcing vendors.

[43] *Supra* note 38.
[44] *Id.*

81. Consistent with Bain's well-documented pattern of cost-driven offshoring, particularly of high wage functions such as IT, these practices extended to PowerSchool's cybersecurity staff under Bain's direction.

82. Though hiring in India was planned across all PowerSchool business units to strengthen Research and Development (R&D), the expansion specifically targeted key technology roles such as Data Scientists and Artificial Intelligence/Machine Learning (AI/ML) experts.[45]

83. These positions were intended to support Bain's goals to also integrate AI functionality into PowerSchool's educational software.

84. In these early discussions, initial and subsequent due diligence assessment, and subsequently through the Merger Agreement, Bain Capital gained comprehensive visibility into PowerSchool's operations, including privileged, non-public insight to internal financials, cybersecurity and technology operations, human resources, product-road-maps, and cost-structure data well before any formal bid.

F. BAIN SIGNS MERGER AGREEMENT WITH POWERSCHOOL

85. Bain's strategic discussions and business planning with PowerSchool culminated in a Merger Agreement signed June 6, 2024. From that point forward, PowerSchool was required to consult Bain Capital prior to making any changes to operational, cybersecurity, and financial decisions, such as restrictions on hiring, engaging, or terminating any "current or former director, officer, employee, or individual independent contractor" above a certain base compensation, as well as restrictions on incurring capital expenses above a certain amount.[46] Furthermore, Bain

[45] Sreeradha Basu, *PowerSchool aims to grow India employee base to 2000 in 3-5 years,* Economic Times (Jan. 9, 2024), https://economictimes.indiatimes.com/industry/services/education/powerschool-aims-to-grow-india-employee-base-to-2000-in-3-5-years/articleshow/106666545.cms.

[46] Agreement and Plan of Merger between BCPE Polymath Buyer, Inc., BCPE Polymath Merger Sub, Inc. and PowerSchool Holdings, Inc. (June 6, 2024), https://www.sec.gov/Archives/edgar/data/1835681/000119312524157845/d846178dex21.htm.

secured veto rights well before the merger officially closed on October 1, 2024, granting Bain strategic control over PowerSchool's key decisions months in advance. As a result, Bain began shaping the company's operations long before the December 2024 data breach, through the control it took both during merger discussions as well as when the Merger Agreement was signed but prior to full acquisition of PowerSchool.

86. Section 6.1 of the Merger Agreement barred PowerSchool from making any capital expenditure over $5 million, entering or amending material vendor contracts, or implementing "any material changes" in compensation or headcount without Bain's written consent between signing on June 6, 2024, and closing on October 1, 2024. This gave Bain *de facto* operational control four months before legal ownership transferred.

87. The $5.6 billion acquisition of PowerSchool was financed through extensive private credit commitments, with several leading firms, including Ares Capital Management, HPS Investment Partners, Blackstone Alternative Credit Advisors, and Blue Owl Credit Advisors, providing the debt financing necessary to complete the $5.6 billion transaction.

88. The $5.6 billion acquisition was financed with approximately $3 billion in secured private credit debt, collateralized by PowerSchool's assets. To offset Bain's debt heavy structure and needing margin expansion to meet its obligations, Bain resorted to cost cutting — including labor reductions and offshore outsourcing — which were central to Bain's control strategy well before the merger formally closed.

89. Ultimately, Bain loaded roughly $3 billion in debt—more than half of PowerSchool's $5.6 billion enterprise value—onto the business,[47] effectively compelling aggressive expense reductions to service the debt.

[47] *Banks and private credit firms compete for PowerSchool buyout,* PRIVATE EQUITY WIRE (MAY 22, 2024), https://www.privateequitywire.co.uk/banks-and-private-credit-firms-compete-for-powerschool-buyout/.

90. As a result, even prior to October 1, 2024, when the deal closed and PowerSchool became "a wholly-owned subsidiary" governed by a Bain-controlled board, Bain began exercising its influence over staffing, spending, and operational priorities. These early steps and control laid the groundwork for the subsequent cost-cutting measures and offshore expansion that contributed directly to the vulnerabilities exploited in the December breach.

91. On October 1, 2024, Bain Capital officially took control. It immediately stripped the PowerSchool's existing board, replacing them with Bain trusted operators and advisors to ensure that every decision and operations were now under Bain Capital's control.[48]

92. The sweeping resignation of PowerSchool's prior directors, detailed in the October 1, 2024, Form 8-K, underscores the depth of Bain Capital's takeover. With the merger's closing, every board seat was handed to individuals tied to Bain-controlled entities, leaving no question that Bain seized full command, and now had full control of the entire board.

93. PowerSchool Chief Executive Officer ("CEO") Hardeep Gulati made clear that he intended on working closely with the management at Bain in management and expansion of the company. In the announcement regarding the merger, Gulati cited Bain's capacity to support AI integration as motivation for the merger, claiming "[w]ith Bain Capital's support, PowerSchool will have access to additional resources and the flexibility to deliver even more growth and innovation, particularly with PowerBuddy, our generative AI platform, and scale our global reach in helping schools personalize education for every student journey."[49]

---

[48] PowerSchool Holdings, Inc(Form 8-K) (Oct. 1, 2024), https://www.sec.gov/Archives/edgar/data/1835681/000119312524230179/d94063d8k.htm (last accessed July 21, 2025).

[49] Press Release, PowerSchool to be Acquired by Bain Capital in $5.6 Billion Transaction, BAIN CAPITAL (June 7, 2024), https://www.baincapital.com/news/powerschool-be-acquired-bain-capital-56-billion-transaction.

94. This announcement underscores that the merger was an active and coordinated strategy with Bain, driving AI integration, and scaling the "global reach," with Bain actively managing and beginning its operations prior to the deal closure.

95. The timing of PowerSchool's announcement of the general availability of its latest PowerBuddy™ AI products—PowerBuddy™ for Learning Student Assistant and PowerBuddy™ for Data Analysis—on June 21, 2024, just two weeks after the Merger Agreement was signed, also underscores Bain's involvement in the strategy and development of these AI tools.[50]

G. BAIN FAILED TO ASSESS AND MITIGATE DATA-BREACH RISKS

96. Even before entering into the Merger Agreement with PowerSchool, Bain was fully aware that data security was a material, important aspect of PowerSchool's business, and that a breach of data security was a key enterprise risk for PowerSchool. Such knowledge is evident in Article 1.1 and 3.17 of the June 6, 2024 Merger Agreement.

97. Article 1.1 of the Merger Agreement provides a definition for "Data Protection Obligation":[51]

> (kk) "**Data Protection Obligations**" means all (i) federal, state, provincial, municipal, local or foreign Laws, (ii) contractual obligations of the Company and its Subsidiaries, and (iii) written privacy policies, terms of use, or other public representations of the Company or any of its Subsidiaries, in each case, to the extent related to privacy, information security, data protection, data breach notification, cross border data transfers, targeted advertising, online marketing

[50] Press Release, *PowerSchool Announces New Contextual AI Solutions, Personalized for Amplifying Student Engagement and Democratizing Data Access*, BUSINESS WIRE (June 21, 2024), https://www.businesswire.com/news/home/20240620423198/en/PowerSchool-Announces-New-Contextual-AI-Solutions-Personalized-for-Amplifying-Student-Engagement-and-Democratizing-Data-Access.

[51] *See supra* note 46 at 6.

> activities, the tracking or monitoring of online activity, or Processing of Personal Information.

98. And in Article 3.17, Bain required PowerSchool to warrant, among other things, that it had "materially complied with all applicable Data Protection Obligations" in the three preceding years:[52]

> *3.17 Data Privacy*.
>
> (a) Except as would not reasonably be expected to have, individually or in the aggregate, a Company Material Adverse Effect, the Company and its Subsidiaries have, currently and during the past three (3) years, materially complied with all applicable Data Protection Obligations and have adopted and published privacy policies on their websites that accurately describe their Processing of Personal Information.
>
> (b) Except as would not reasonably be expected to have, individually or in the aggregate, a Company Material Adverse Effect, the Company and its Subsidiaries have implemented and maintain a written information security program comprising commercially reasonable administrative, technical and physical safeguards.
>
> (c) Except as would not reasonably be expected to have, individually or in the aggregate, a Company Material Adverse Effect, to the Knowledge of the Company, neither the Company nor any of its Subsidiaries have experienced any Security Incident; or received any claim alleging that the Company or any of its Subsidiaries has violated any Data Protection Obligation or, to the Knowledge of the Company, been the subject of any governmental investigation or enforcement action making such an allegation in the past three (3) years.

[52] *Id.*

> (d) Except as would not reasonably be expected to have, individually or in the aggregate, a Company Material Adverse Effect, neither the Company nor any of its Subsidiaries sell, or have sold, Personal Information collected from or regarding students or children under the age of thirteen (13) in contravention of applicable Data Protection Obligations.
>
> (e) Except as would not reasonably be expected to have, individually or in the aggregate, a Company Material Adverse Effect, neither the Company nor its Subsidiaries have engaged in any targeted online advertising or created profiles for non-educational purposes based on students' Personal Information in contravention of Data Protection Obligations.

99. Despite its knowledge of the critical importance of data security, Bain failed to properly assess the risks of potential data breaches associated with PowerSchool's offshore expansion.

100. Bain also failed to mitigate such risks by designing and implementing adequate systems and procedures to prevent hackers from infiltrating PowerSchool's data storage facilities.

H. BAIN DIRECTED LAYOFFS AND OFFSHORE EXPANSION

101. In March 2024, briefly after PowerSchool announced its plan to increase offshore hiring, PowerSchool initiated a wave of layoffs that eventually affected approximately 5% of its workforce, including many U.S.-based employees with over 20 years of experience at the company.[53] [54] [55]

---

[53] u/InstructionNeither98, REDDIT (r/Schoology), *PowerSchool laid off 5% of its workforce last week…*, (2024), https://www.reddit.com/r/Schoology/comments/1ewqljn/powerschool_laid_off_5_of_its_workforce_last_week/.

[54] PowerTool (@PowerTool_), X (Aug. 13, 2024 11:49PM PST), https://x.com/powertool_/status/1823612984624664959.

[55] Anonymous, Employee Review: PowerSchool Group, GLASSDOOR (Aug. 19, 2024), https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW90209904.htm.

102. The timing of these layoffs, occurring several years after Bain's initial discussions with PowerSchool regarding a potential acquisition, support the conclusion that cost-reduction planning was already underway in anticipation of Bain's acquisition.

103. Three months after the acquisition announcement, PowerSchool initiated further layoffs in August 2024, during which time Bain oversaw all major decisions and directed the layoffs.

104. Employee accounts on social media, such as Reddit and X, and job review sites, such as Indeed and Glassdoor, linked the layoffs directly to Bain Capital's financial expectations in the wake of the acquisition. According to an inside source, PowerSchool reported a quarterly earnings per share of $0.23, missing the consensus estimate of $0.24 per share, by one penny per share.[56] [57]

105. PowerSchool's former employees have commented on social media regarding Bain's role in the layoffs at PowerSchool, as well as the increased offshoring. For example, a former Product Engineer at PowerSchool posted on Glassdoor regarding a "[l]arge scale layoff" and warned that the company was shifting toward outsourcing, stating: "it is a general trend to outsource all the jobs to off shore [sic]… now it's shifting to support and product management."[58] A former employee echoed this sentiment, writing that the "Company is also clearly shifting to an India-based workforce at the expense of US-based employees."[59] One reviewer bluntly warned

[56] *PowerSchool Announces Second Quarter Financial Results*, BUSINESS WIRE (Aug. 19, 2024), https://www.businesswire.com/news/home/20240808373822/en/PowerSchool-Announces-Second-Quarter-Financial-Results.

[57] Wyatt Gaylor (@wyattg), X (Aug. 24, 2024 8:09AM PST), https://x.com/wyattg/status/1823738764730229073.

[58] Anonymous, Employee Review: PowerSchool Group, GLASSDOOR (Aug. 19, 2024), https://www.glassdoor.com/Reviews/Employee-Review- PowerSchool-Group-E1110566-RVW90216913.htm.

[59] Anonymous, Employee Review: PowerSchool Group, GLASSDOOR (Aug. 20, 2024), https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW90258225.htm.

U.S.-based employees: "if you are in the US working for PS… you will get laid off within 6 months as your job responsibilities get moved [offshore]."[60] Others described how the company's culture had changed under new ownership, stating that what "started as a mission-driven company to help every student achieve quickly became a profit-first march towards ed-tech domination."[61]

106. Job postings dated shortly after the June 2024 acquisition announcement corroborate Bain's outsourcing of roles at PowerSchool, specifically IT and tech-related roles across the globe.

107. These additional layoffs and outsourcing decisions following the formalization of the merger reflect Bain's continuing pressure to meet financial targets and implement aggressive cost-cutting measures. This also aligns with Bain's strategy of consolidating operations and reducing labor costs post-acquisition.[62]

108. A significant portion of this Bain-led outsourcing was done through contracting with Movate, Inc., an outsourcing company. After Bain's signing of merger documents, Movate began advertising in July 2024 for additional staff in the Philippines to service PowerSchool's account. Consistent with Bain's veto rights and its well-documented strategy of cost-reduction through offshoring, this expansion proceeded only with Bain's knowledge, approval, and direction.

I. BAIN'S CONTROL POST-MERGER AND ITS IMPACT ON CYBERSECURITY AND STAFFING

109. After the merger, Bain had complete control over PowerSchool's expenditures and staffing decisions, as well as significant influence prior to the merger.

---

[60] Anonymous, Employee Review: PowerSchool Group, GLASSDOOR (Oct. 23, 2024), https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW92208768.htm.

[61] Anonymous, Employee Review: PowerSchool Group, GLASSDOOR (Sept. 12, 2024), https://www.glassdoor.com/Reviews/Employee-Review-PowerSchool-Group-E1110566-RVW90973925.htm.

[62] PowerTool (@PowerTool_), X (Aug. 13, 2024 11:49PM PST), https://x.com/powertool_/status/1823612984624664959.

Once Bain's acquisition took PowerSchool private, it had complete ownership and control over PowerSchool's decisions, including cybersecurity and security strategies and staffing.

110. Since Bain's business model was to take dividends or profits from the purchased business to pay its investors, any additional money spent on cybersecurity was money that could not have been provided to Bain and its investors. This helped Bain ensure PowerSchool met certain return-on-investment targets on a quarterly basis that might not have occurred if it made significant (but clearly required) investments in cybersecurity.

111. Additionally, the significant debt that PowerSchool took on for the merger (the leveraged buyout) added a significant amount of interest PowerSchool now had to pay on a regular basis, further increasing its costs and requiring further cost-cutting, of which cybersecurity and IT were prime targets as they did not immediately increase revenue.

112. PowerSchool's leveraged buyout under Bain's control led to a marked reduction in staffing.

J. AFTER ACQUIRING POWERSCHOOL, BAIN FAILED TO IMPLEMENT THE BASIC SECURITY MEASURES NECESSARY TO PROTECT THE INFORMATION BAIN AND POWERSCHOOL HAD IN THEIR POSSESSION

113. After signing the Merger Agreement, and conducting extensive due diligence, Bain became closely involved with PowerSchool's operations, and ultimately became an owner, closely overseeing and controlling all operations of PowerSchool, including controlling its newly appointed board.

114. Bain holds itself out as a sophisticated, tech-focused investor with the expertise to guide companies through digital transformation. Bain thus had responsibility, authority, and expertise to ensure that PowerSchool implemented basic,

industry-standard safeguards – including requiring all of their vendors and employees to use a multifactor authentication.

115. Having studied the company for over two years before the merger and then having taken control of the company – Bain knew that failing to implement these elementary precautions would leave millions of students and teachers vulnerable to exactly the kind of breach that occurred here.

K. POWERSCHOOL OUTSOURCES SUPPORT TO MOVATE

116. Movate was a key actor in Bain's rush to offshore and outsource key PowerSchool functions. Movate is a global outsourcing company hired to act an an extension of various companies in the United States and across the globe.

117. From the United States, Movate leverages a global network of over 12,000 employees across 21 locations to provide technical and customer support. When a company contracts to use Movate services (an agency relationship), Movate directs its employees, including employees in the Philippines, on how to fulfill the contract on behalf of that entity on a day-to-day basis to ensure consistency across its 21 locations.

118. Movate has also developed and directed day-to-day data security practices across its offices. For example, Movate's Associate Vice President and Head of Information Security has stated that Movate is certified as compliant under the ISO 27001:2013 framework across North America, Asia (including offices in the Philippines), Africa, Latin America, and Europe.[63]

119. Movate itself advertised for roles including "Team lead," "Network Operations Engineer," and "Systems Engineer" in the Philippines in 2024.[64] Movate

[63] *Information security at Movate: Assessments and compliance*, Movate, available at https://www.movate.com/information-security-at-movate-assessments-and-compliance/ (last accessed July 29, 2025).

[64] *Careers at Movate Philippines*, Movate, https://www.movate.com/careers-at-movatephilippines/ (archived on Oct. 4, 2024, at http://web.archive.org/web/20241004204953/https://www.movate.com/careers-atmovate-philippines/).

employees with these or similar titles are listed on LinkedIn as providing support for PowerSchool.[65]

120. An individual by the name of Rayson Cruz appears to be one such employee. He is listed as a Movate Team Leader in the Philippines and was assigned to provide technical support on behalf of PowersSchool.[66] Mr. Cruz, and likely many other Movate employees, had access to every single student and teacher record in the PowerSchool Student Information System (SIS).[67] As a result, and as described more fully below, his compromised credentials were all that hackers needed to exfiltrate Plaintiffs' and Class Members' data.[68]

L. CYBERCRIMINALS EASILY EXPORT SENSITIVE RECORDS FROM POWERSCHOOL, POSING AN ONGOING RISK TO MILLIONS OF TEACHERS AND FAMILIES

121. Despite PowerSchool's repeated assurances concerning data security, PowerSchool's systems were easily breached, exposing detailed and highly sensitive records for tens of millions of students, parents, and teachers.

---

[65] *See, e.g.*, *Maryan Medua*, LinkedIn, available at https://www.linkedin.com/in/maryan-medua-902aa6328/?originalSubdomain=ph (last visited July 29, 2025) (noting that employee worked at Movate and served as "Technical Support Engineer" starting in September 2024 and worked on PowerSchool SIS).

[66] "Remote Support connection from the IP address of 91[.]218[.]50[.]11 with the user 'Rayson Cruz' is one of the primary indicators of compromise." PowerSchool Incident FAQs, North Dakota Information Technology. A Rayson Cruz based in the Philippines is listed as a Team Leader for Movate on LinkedIn. *Rayson Cruz*, LinkedIn, available at https://www.linkedin.com/in/rayson-cruz-3425bb292/.

[67] CrowdStrike Services, *Investigation Report, prepared for PowerSchool Group, LLC* (Feb. 28, 2025) at 5, available at https://www.powerschool.com/wp-content/uploads/2025/03/PowerSchool-CrowdStrike-Final-Report.pdf ("CrowdStrike Report").

[68] "Remote Support connection from the IP address of 91[.]218[.]50[.]11 with the user 'Rayson Cruz' is one of the primary indicators of compromise." PowerSchool Incident FAQs, North Dakota Information Technology.

1. AN UNAUTHORIZED ACTOR USING A LONE MOVATE EMPLOYEE'S CREDENTIALS EXFILTRATED THE DATA WITHOUT SOUNDING ANY ALARMS.

122. On January 7, 2025, PowerSchool announced that it had been the subject of a Data Breach.

123. In a statement posted on its website, PowerSchool stated that, "[o]n December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of certain personal information from PowerSchool SIS environments through one of [its] community-focused customer support portals, PowerSource."[69] PowerSchool claimed that the Data Breach occurred between December 19 and December 28, 2024.[70]

124. PowerSchool maintained that only "certain" personal information was exfiltrated, that the Breach occurred only in December 2024, and, later, that the "incident" had been "contained."[71]

125. But, the reality was much worse. The PII of millions of tens of millions of teachers and students (and their families) was exfiltrated, with there being signs of unauthorized access to this Data as early as August 2024.

126. In the months following the Data Breach, several revelations have shed light on the shocking nature, timing, and extent of the Breach—which PowerSchool has deliberately minimized—as well as PowerSchool's many failures to prevent the Data Breach.

---

[69] PowerSchool, *Notice of Data Breach for Individuals in the United States*, available at https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/ (last visited July 17, 2025) ("Breach Notice").

[70] NAPS District, *PowerSchool Data Breach Update*, Colegrove Park Elementary School (Jan. 9, 2025), available at https://ces.napsk12.org/o/cpes/article/1955718.

[71] Anna Merod, *PowerSchool data breach possibly exposed student, staff data*, K-12 Dive (Jan. 9, 2025), available at https://www.k12dive.com/news/powerschool-data-breach-cybersecurity-incident/736974/.

127. For instance, and remarkably, the entire Breach was purportedly carried out using the compromised credentials of a single Movate employee.

128. On December 29, 2024, PowerSchool retained the cybersecurity technology firm, CrowdStrike Services ("CrowdStrike"), "to provide investigative services and to assess the scope and extent of unauthorized third party ('Threat Actor') activity in the PowerSchool environment."[72] On February 28, 2025, CrowdStrike released its report (the "CrowdStrike Report"), detailing the results of its investigation.[73] The CrowdStrike Report concludes that the unauthorized third party—or "Threat Actor"—that ultimately exfiltrated the Data from PowerSchool did so using credentials belonging to a single PowerSchool "support user."[74] As discussed further below, this "Threat Actor" was an individual associated with "ShinyHunters," a notorious cybercriminal group.

129. The CrowdStrike Report continues:

> **The Threat Actor performed Maintenance Remote Support operations in PowerSource to gain access to PowerSchool customers' SIS data.** Between December 19, 2024, at 19:43:14 UTC, and December 28, 2024, at 06:31:18 UTC, the Threat Actor performed Maintenance Remote Support operations in PowerSource, which enabled the Threat Actor to access the individual customer organizations' SIS instances. At 19:43:37 UTC, the Threat Actor initiated a Maintenance Remote Support connection to PowerSchool SIS from the same IP address using the compromised support credentials.[75]

[72] CrowdStrike Services, *Investigation Report, prepared for PowerSchool Group, LLC* (Feb. 28, 2025) at 3, available at https://www.powerschool.com/wp-content/uploads/2025/03/PowerSchool-CrowdStrike-Final-Report.pdf ("CrowdStrike Report").
[73] *Id*.
[74] *Id*.
[75] *Id*. at 5 (emphasis in original)

130. PowerSchool has confirmed that the Movate employee's account that was used in the Breach was not protected with multifactor authentication, a failing that is discussed further below.[76]

131. Although CrowdStrike did not identify the "support user" whose credentials were compromised, it appears that the compromised account belonged to a Movate employee with the username "Rayson Cruz," who has worked for Movate in the Philippines.[77]

132. Mr. Cruz appears to have had full access to "PowerSchool customers' SIS data," [78] *i.e.*, the PII (including SSNs, names, addresses, medical information, and more) of tens of millions of students, parents, and teachers.

133. Making matters worse, the Movate employee had the capability to not only access this Data, but also to exfiltrate it, and to do so without raising any alarms at PowerSchool. As reported by CrowdStrike, "[b]etween December 19, 2024, at 23:02:54 UTC, and December 23, 2024, at 08:04:45 UTC, the Threat Actor exfiltrated data from the Teachers and Students tables of the PowerSchool SIS instances for certain PowerSchool customers."[79] PowerSchool, however, did not "become aware" of this "unauthorized exfiltration" until December 28, 2024.[80]

---

[76] Zach Whittaker, *Malware stole internal PowerSchool passwords from engineer's hacked computer*, TechCrunch (Jan. 17, 2025), available at https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/.

[77] "Remote Support connection from the IP address of 91[.]218[.]50[.]11 with the user 'Rayson Cruz' is one of the primary indicators of compromise." PowerSchool Incident FAQs, North Dakota Information Technology. As described above, there appears to be no publicly-listed resident in the United States by this name.

[78] CrowdStrike Report at 5.

[79] *Id.*

[80] Breach Notice.

2. SUSPICIOUS ACTIVITY BEGAN FOUR MONTHS BEFORE THE BREACH, BUT POWERSCHOOL ONLY LEARNED THAT ITS SYSTEMS WERE BREACHED WHEN IT WAS BEING EXTORTED IN DECEMBER 2024.

134. The CrowdStrike Report contained another shocking revelation: beginning on August 16, 2024, PowerSchool logs showed that an unknown actor successfully accessed the PowerSchool portal, using the Movate employee's compromised support credentials.[81]

135. This demonstrates that there was an unknown individual, or unknown individuals, accessing PowerSchool's customers' data at least four months before the publicly announced Data Breach. Yet, it appears that PowerSchool had no prior knowledge of this activity.

136. And PowerSchool did not notice when on September 4, 2024, a then unknown individual reportedly gained unauthorized access to PowerSchool's network, and obtained student and teacher data belonging to one of PowerSchool's customers from PowerSchool's network.[82]

137. Moreover, PowerSchool did not notice when an unknown actor not only accessed but downloaded sensitive information for tens of millions of students and teachers in December 2024. Instead, PowerSchool only learned of the Data Breach when, on December 28, 2024, it received a ransom demand of $2.85 million in Bitcoin, threatening that if PowerSchool did not pay, the Data would be leaked.[83]

138. In sum, PowerSchool did not notice when an unknown actor accessed its customers' SIS data in August 2024, or September 2024, nor when an unknown actor

---

[81] CrowdStrike Report at 5.

[82] *United States v. Lane*, No. 25-cr-40015, ECF No. 1 (D. Mass. May 20, 2025).

[83] Anna Merod, *College student charged in connection with PowerSchool data breach*, K-12 Dive (May 21, 2025), available at https://www.k12dive.com/news/college-student-charged-in-connection-with-powerschool-data-breach/748747/.

exfiltrated millions of records over the course of four days in December 2024. Instead, PowerSchool only learned of the Data Breach when it was being extorted.

3. DEFENDANTS' FAILINGS COMPROMISED THE HIGHLY SENSITIVE INFORMATION OF MILLIONS OF STUDENTS, PARENTS, AND TEACHERS.

139. According to multiple sources, ShinyHunters "claimed to have stolen the data of 6,505 school districts in the US, Canada, and other countries," meaning that the Breach "impacted 62,488,628 students and 9,506,624 teachers."[84]

140. PowerSchool, however, has not confirmed whether these figures are accurate.[85] In fact, PowerSchool has "repeatedly declined to say how many schools and individuals are affected," despite conceding that it has already "identified the schools and districts whose data was involved in this incident."[86]

141. All told, the Data Breach appears to "be the largest single breach ever of American schoolchildren's data."[87]

142. As discussed herein, the PowerSchool SIS houses a myriad of highly sensitive information, including SSNs, dates of birth, addresses, learning disabilities and IEPs, disciplinary records, child custody information, and credit card information. *See infra* ¶ 18.

143. PowerSchool's notices indicate that the stolen Data was highly sensitive,[88] stating that the compromised information included: names, contact information, date

[84] Lawrence Adams, *PowerSchool hacker claims they stole data of 62 million students*, Bleeping Computer (Jan. 22, 2025), available at https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/.

[85] Carly Page, *What PowerSchool won't say about its data breach affecting millions of students*, TechCrunch (March 10, 2025), available at https://techcrunch.com/2025/03/10/what-powerschool-isnt-saying-about-its-massive-student-data-breach/.

[86] *Id.*

[87] Tim Starks, *Massachusetts man will plead guilty in PowerSchool hack case*, CyberScoop (May 20, 2025), available at: https://cyberscoop.com/massachusetts-man-will-plead-guilty-in-powerschool-hack-case/.

[88] Page, *supra* n.37.

of birth, limited medical alert information, Social Security Number, and other related information.[89]

144. As multiple affected school districts have reported, the "other related information" that was compromised includes, for example:

- medical diagnoses (including mental health information) and medical conditions;[909192]
- free meal statuses;[93]
- legal alerts, including custody agreements, restraining orders, and other legal information[9495]; and
- special education designations.[96]

4. POWERSCHOOL PAID A RANSOM, BUT THE STOLEN DATA IS STILL CIRCULATING.

145. PowerSchool ultimately paid a ransom to the threat actor.[97] PowerSchool then claimed to have "watched a video of the hacker deleting the data,"[98] and declared

---

[89] Breach Notice.
[90] Carly Page, *PowerSchool begins notifying students and teachers after massive data breach*, TechCrunch (Jan. 28, 2025), available at https://techcrunch.com/2025/01/28/powerschool-begins-notifying-students-and-teachers-after-massive-data-breach/.
[91] *Id.*
[92] Suzanne Smalley, *PowerSchool breach exposed special education status, mental health data and parent restraining orders*, The Record (Feb. 11, 2025), available at https://therecord.media/powerschool-breach-exposed-special-ed-status-mental-health-data.
[93] Page, *supra* n.42.
[94] *Id.*
[95] *Id.*
[96] Smalley, *supra* n.44.
[97] PowerSchool, *PowerSchool Cybersecurity Incident* (May 7, 2025), https://www.powerschool.com/security/sis-incident.
[98] WSOCTV.com, *PowerSchool says hacker deleted student, teacher records obtained in breach* (May 6, 2025), available at https://www.wsoctv.com/news/local/powerschool-says-hacker-deleted-student-teacher-records-obtained-breach/6OUM3C3RFNE6JLEHQ26UTW7YJQ/.

that "the incident is contained" and that it "d[id] not anticipate the data being shared or made public."[99]

146. Despite PowerSchool purportedly paying the ransom, however, multiple school districts have since been approached with extortion demands, indicating that the stolen Data is still in the hands of cybercriminals. On May 7, 2025, PowerSchool posted a statement on its website, explaining that a threat actor "has reached out to multiple school district customers in an attempt to extort them using data from the previously reported December 2024 incident."[100] PowerSchool continued: "As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to [PowerSchool]."[101]

147. This is no longer a risk, but a reality. By all indications, either the Data was never deleted in the first place, or other copies of it were made, as the Data—which can be made available for sale or used to extort members of the Class— is likely available on the dark web.[102] The threats poised to students and teachers therefore remain ongoing.

---

[99] Merod, *supra* n.24.

[100] PowerSchool, *PowerSchool Cybersecurity Incident* (May 7, 2025), https://www.powerschool.com/security/sis-incident.

[101] *Id.*

[102] The "dark web" is a term for websites that are only accessible via The Onion Router ("TOR") network. The term onion routing is used because data is encrypted in layers like an onion. Each relay in the network peels away a layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data. When using the TOR network, a user's IP address is masked, and their internet traffic is routed through a series of relays before reaching the destination. This makes it difficult for websites, internet service providers, or third parties to track the user's real IP address or browsing activity. The term dark web is used because these websites cannot be found via traditional means. Only via onion routing can one access a site on the dark web. Since the dark web can only be accessed via onion routing, and the process of onion routing hides the origin of any packet, the dark web inherently has greater anonymity than traditional websites.

148. This result was predictable because hackers like ShinyHunters lie.[103] PowerSchool,[104] the CISA,[105] the FTC,[106] the NSA[107] and countless other agencies and experts[108] all recognize this fact.

149. There is even more reason to think that paying a ransom would not contain the harm to teachers and students here because, even if there was a reason to trust the person PowerSchool understood to be "ShinyHunters," (one person's word does not matter when ShinyHunters is a decentralized network of many hackers with different agendas, motivations, and capacities to do harm to Plaintiffs and Class Members.

150. As further reported by Education Week:

> While there are only a couple of reports so far of school district customers receiving extortion threats, there could be many more to come, said Doug Levin, a school cybersecurity expert and the national director of the K12 Security Information Exchange. All schools affected by the initial data breach need to be prepared, he said. "We may have just heard about the

---

[103] Mathew J. Schwartz, *PowerSchool's Breach Fallacy: Paying Criminals for Promises*, Bank Info Security (Jan. 10, 2025), available at https://www.databreachtoday.eu/blogs/powerschools-breach-fallacy-paying-criminals-for-promises-p-3793 (collecting numerous examples).

[104] PowerSchool, *PowerSchool: A Leader in Responsible AI for Education* at 14, available at https://go.powerschool.com/rs/861-RMI-846/images/Responsible_AI_Cybersecurity_Report.pdf?version=0 (last visited July 23, 2025).

[105] CISA, *Ransomware*, available at https://www.cisa.gov/sites/default/files/publications/Ransomware%2520General%2520Security%2520Postcard%25206.23.2021_508c.pdf (last visited July 18, 2025).

[106] FTC, *Ransomware*, available at https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/ransomware (last visited July 18, 2025).

[107] CISA, NSA, FBI, and Multi-State Information Sharing & Analysis Center, *#StopRansomware Guide*, available at https://media.defense.gov/2023/May/23/2003227891/-1/-1/0/CSI-StopRansomware-Guide.PDF (last visited July 23, 2025).

[108] *Don't Pay The Ransom! What the Experts Say About Responding to Extortion*, Macrium Blog (May 15, 2024), available at https://www.macrium.com/blog/dont-pay-ransom-what-experts-say-about-responding-to-extortion (collecting sources); *see also* Sara Brown, *How to respond to a ransomware attack: Advice from a federal agent*, MIT (Jan. 19, 2022), available at https://mitsloan.mit.edu/ideas-made-to-matter/how-to-respond-to-a-ransomware-attack-advice-a-federal-agent; Matt Martin, *Beware of ransomeware. And don't pay the ransom!*, University of Michigan (Aug. 16, 2018), available at https://michigan.it.umich.edu/news/2018/08/16/beware-of-ransomware/.

tip of the iceberg, and there may be more extortion demands coming," Levin said.[109]

151. Individuals whose Data was exposed are also being targeted. For example, on May 8, 2025, the Sampson County Public Schools in North Carolina warned families and teachers that several schools and educators across the state had "received email messages within the past week from threat actors claiming to have access to the same student and teacher data" from the Data Breach.[110] The warning went on to advise teachers and families not to open suspicious links in any emails claiming to come from ShinyHunters.[111]

5. MATTHEW LANE PLEADS GUILTY TO HIS ROLE IN THE BREACH, BUT SHINYHUNTERS REMAINS AT LARGE AND STILL HAS THE DATA.

152. On May 20, 2025, Matthew Lane ("Lane"), a 19-year-old student at Assumption University in Worcester, Massachusetts, pled guilty to hacking into two companies, "Victim 1" and "Victim 2," the latter of which is understood to be PowerSchool.[112]

---

[109] Lauraine Langreo & Arianna Prothero, *PowerSchool Paid a Hacker's Ransom. Now Cyber Criminals Are Threatening Schools*, EducationWeek (May 8, 2025), available at https://www.edweek.org/technology/powerschool-paid-a-hackers-ransom-now-cyber-criminals-are-threatening-schools/2025/05.

[110] Valerie Newton, *Update on New PowerSchool Data Breach and Ongoing Protection Measures*, Sampson County Schools (May 8, 2025), available at https://www.sampson.k12.nc.us/article/2199993.

[111] *Id.*

[112] PowerSchool is not referenced by name in either the Charging Document or plea agreement. However, multiple outlets have reported that sources confirmed to them that PowerSchool was the "software and cloud storage company that served school systems in the United States, Canada, and elsewhere" that is referenced in the Charging Document. *See, e.g.*, Starks, *supra* n.39; Kevin Collier, *19-year-old accused of largest child data breach in U.S. agrees to plead guilty to federal charges*, NBC News (May 20, 2025), available at https://www.nbcnews.com/tech/security/alleged-hacker-largest-breach-us-childrens-data-agrees-plead-guilty-rcna207963.

153. The Charging Document[113] against Lane, filed by the United States Attorney's Office for the District of Massachusetts, states that Lane used the Movate employee's credentials to first gain unauthorized access to PowerSchool's computer network on September 4, 2024.[114]

154. The Charging Document further states that Lane then leased a computer server in Ukraine on or around December 19, 2024 and, starting on December 20, 2024, caused the Data to be transferred to this server in Ukraine.[115]

155. According to the Charging Document, Lane also conspired to extort Victim 1, another entity whose confidential customer information had been stolen.[116]

156. Critically, the Charging Document makes clear that Lane did not act alone. Instead, at least with respect to the crimes against Victim 1, the Charging Document specifies that Lane acted with one unnamed coconspirator, if not more.[117] That accomplice, or set of accomplices, remains at large.

157. Although not explicitly addressed in the Charging Document, there are multiple indications that, with respect to Victim 2—i.e., PowerSchool—Lane worked with ShinyHunters, a decentralized hacking group that is described below.

158. First, the Charging Document suggests that Lane had a coconspirator (or multiple) in carrying out the Data Breach. In particular, the Charging Document explicitly states that Lane himself sent the ransom demand to Victim 1.[118] However, for Victim 2, the Charging Document makes no such allegation, and instead simply states that "[PowerSchool] received a ransom demand."[119] Indeed, neither the Charging

---

[113] *United States v. Lane*, No. 25-cr-40015, ECF No. 1 (D. Mass. May 20, 2025) (the "Charging Document").
[114] *Id.* ¶¶ 10-11.
[115] *Id.* ¶¶ 12-13.
[116] *Id.* ¶ 6.
[117] *Id.* ¶ 9.
[118] *Id.* ¶ 9.
[119] *Id.* ¶ 14.

Document nor Lane's plea agreement[120] indicate that Lane sent a ransom demand to PowerSchool, nor that he appeared on camera to delete the Data, as PowerSchool claims. It stands to reason, then, that someone other than Lane carried out these acts.

159. Second, as noted above, extortion demands made to school districts and educators in May 2025 appear to have come from ShinyHunters. Similarly, a New York school district reported that the State Education Department's chief privacy officer notified the district that ShinyHunters members were "the threat actors responsible for the December 2024 PowerSchool breach."[121]

160. Finally, Lane has been reported to be "affiliated" with ShinyHunters.[122]

161. Although Lane may have been apprehended, ShinyHunters has not been held to account. Worse yet, as the recent extortion demands and ShinyHunters' own tactics, discussed more below, indicate, ShinyHunters still has the Data and fully intends to use it.

162. Thus, despite Lane's plea agreement, Plaintiffs and Class Members continue to face at least three very real harms: ShinyHunters (1) continuing to use the stolen Data to extort Plaintiffs and Class Members, (2) selling or releasing Plaintiffs' and Class Members' Data on the dark web, and/or (3) using the Data itself to otherwise harm Plaintiffs and Class Members.

M. THE BREACH WAS FORESEEABLE

163. The Data Breach was not the first time that hackers used compromised credentials to access troves of data. It was also not the first time that the K-12 education sector had been targeted by hackers, nor the first time that ShinyHunters used these tactics. Defendants therefore knew or should have known of the risks posed by hackers like ShinyHunters, but failed to protect against them.

---

[120] *Lane*, ECF No. 2.

[121] Media Specialist, *Important Cybersecurity* Alert, Roosevelt Union Free School District (May 14, 2025), available at https://www.rooseveltufsd.org/article/2213612.

[122] Starks, *supra* n.39; *Windows Server 2025 Vulnerable in Active Directory*, SANS (May 23, 2024), available at https://www.sans.org/newsletters/newsbites/xxvii-40/.

1. LEADING UP TO THE DATA BREACH, DATA SECURITY INCIDENTS RESULTING FROM COMPROMISED CREDENTIALS WERE WIDESPREAD.

164. Leading up to the Data Breach, the K-12 education sector was a repeated target of data breach attacks. An increased reliance on new technology in the wake of COVID-19 led to more data being collected about students.[123] In turn, as this new technology spread, hackers developed a playbook that led to a rise in data security incidents.[124] Over 1,300 incidents occurred between 2018 and 2021 alone.[125]

165. Schools and educational institutions are desirable targets for hackers for multiple reasons, because (1) student and teacher data can be incredibly useful for hackers, (2) institutions may use new, untried technology, and (3) email addresses ending in ".edu" are valuable, among other things.[126]

166. PowerSchool admittedly recognized these risks in representing the following on its website: "PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. ***We strive to continuously maintain reasonable physical, administrative, and technical security measures.***"[127]

167. Many data security incidents involve compromised credentials, both for the K-12 education sector and industry at large. When hackers seek access to large amounts of data through accessing web applications, 86% of incidents involve

---

[123] CISA, *Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity* at 3 (Jan. 19, 2023), available at https://www.cisa.gov/resources-tools/resources/report-partnering-safeguard-k-12-organizations-cybersecurity-threats.

[124] *Id.*

[125] *Id.* at 6.

[126] Cayley Wetzig, *8 Surprising Reasons Hackers Target Schools*, ThriveDX Media (Jan. 18, 2023), 8 Surprising Reasons Hackers Target Schools - ThriveDX .

[127] *Privacy,* PowerSchool (last updated Feb. 2, 2023) https://www.powerschool.com/legal/privacy-2023/.

compromised credentials.[128] More than half of all attacks on critical infrastructure attacks involved the compromise of a user's credentials in 2022.[129]

168. When hackers access sensitive data, their playbook is predictable. The hackers will seek to gain access to, and exfiltrate, as much data as possible.[130] That way, the hackers "can impact the victim's reputation, release sensitive data impacting other users, or disrupt day-to-day operations."[131]

169. Defendants were aware, or at least should have been aware, of these well publicized risks and the harm that could result leading up to the Data Breach. For example, in another high profile breach, ShinyHunters stole terabytes of data from Ticketmaster in June 2024 using compromised credentials that did not require multifactor authentication.[132] And in March 2024, Change Healthcare was hacked using compromised credentials that did also not require multifactor authentication a breach which resulted in the exfiltration of hundreds of millions of Americans' data.[133] School districts around the country have also repeatedly experienced well-publicized data breach incidents resulting from compromised and unprotected credentials.[134]

---

[128] Verizon, *2023 Public Sector Data Breach Investigations Report*, available at https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf.

[129] Matt Kapko, *Valid account credentials are behind most cyber intrusions, CISA finds*, CyberSecurity Dive (July 28, 2023), available at https://www.cybersecuritydive.com/news/valid-credentials-most-intrusions/689118/.

[130] CISA, *CISA Analysis: Fiscal Year 2022 Risk and Vulnerability Assessments* at 15-16 (June 2023), available at https://www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final_508c.pdf.

[131] *Id.* at 16.

[132] Kim Zetter, *Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake*, WIRED (June 17, 2024), available at https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/.

[133] Matt Kapko, *Change Healthcare, compromised by stolen credentials, did not have MFA turned on*, CyberSecurity Dive (April 30, 2024), available at https://www.cybersecuritydive.com/news/change-healthcare-compromised-credentials-no-mfa/714792/.

[134] Brian Bradley, *Combating the Rise of the K-12 Cyberattack*, AASA (Feb. 1, 2024), available at https://www.aasa.org/resources/resource/combating-rise-of-k-12-cyberattack.

2. SHINYHUNTERS IS A NOTORIOUS HACKING GROUP THAT USES COMMONLY KNOWN TACTICS.

170. ShinyHunters is a notorious cybercriminal group that became widely known in 2020, gaining attention with high-profile data breaches.[135,136] ShinyHunters was first widely known for selling 91 million user records from the Indonesian e-commerce platform Tokopedia on the dark web.[137] According to Forbes, "[i]n just the first two weeks of May 2020, a hacker, known only as ShinyHunters, offered an astonishing 200 million stolen data records for sale on the dark web. Not repurposed data from old breaches, but fresh to the market and, therefore, very valuable. The surprising thing is that, until then, nobody had even heard of ShinyHunters."[138]

171. In 2020 alone, ShinyHunters was selling the following data batches on the dark web:[139]

Vakina.com.br — 4.8 million records
Truefire.com — 600,000 records
Havenly.com — 1.3 million records
Drizly.com — 2.4 million records
Proctoru.com — 444,000 records
Scentbird.com — 5.8 million records
Appen.com — 5.8 million (suffered breach in 2017)

---

[135] Lily Hay Newman, *ShinyHunters Is a Hacking Group on a Data Breach Spree*, WIRED (May 21, 2020), available at https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/.

[136] *ShinyHunters, One of the Most Recognized Threat Actors Among the Hacking Community*, WhiteBlueOcean (Feb. 16, 2021), available at https://www.whiteblueocean.com/newsroom/shinyhunters-one-of-the-most-recognised-threat-actors-among-the-hacking-community/.

[137] BugCrowd, Glossary, *ShinyHunters*, https://www.bugcrowd.com/glossary/shinyhunters/ (last visited July 23, 2025).

[138] Davey Winder, *Hacker Gives Away 386 Million Stolen Records on Dark Web—What You Need To Do Now*, Forbes (July 29, 2020), available at https://www.forbes.com/sites/daveywinder/2020/07/29/hacker-gives-away-386-million-stolen-records-on-dark-web-what-you-need-to-do-now-shinyhunters-data-breach/.

[139] *ShinyHunters Offers Stolen Data on Dark Web*, DarkReading (July 28, 2020), available at https://www.darkreading.com/cyberattacks-data-breaches/shinyhunters-offers-stolen-data-on-dark-web.

Homechef.com — 8 million records
Chatbooks.com — 15 million records

172. Since then, ShinyHunters has gained even more notoriety for targeting companies across various sectors, including technology, education, media, and e-commerce, accumulating a significant track record of breaches.

173. ShinyHunters is known for its financially motivated operations, primarily involving the theft and sale of data. They have compromised several companies, such as Pixlr, NitroPDF, and MeetMindful, often leaking the stolen data on hacking forums either for free or for sale.

174. ShinyHunters aims to collect mass amounts of PII and PHI and has disseminated data for sale through a variety of dark web forums. These forums have, at times, been shut down by the FBI, only to reemerge with a different dark web address.[140]

175. ShinyHunters is known for targeting companies with large user bases, like PowerSchool. The group exfiltrates data from these organizations and extorts data breach victims to pay exorbitant sums or risk their data being sold on the dark web.

176. ShinyHunters has targeted well-known platforms and services, typically those with weaker security measures, large user databases, or high-profile reputations. In some instances, ShinyHunters engages in ransom-based attacks, demanding payments to avoid leaking stolen data. Unlike other groups that specialize in ransomware or advanced persistent threat tactics, ShinyHunters focuses on maximizing

[140] Jai Vijayan, *Leak Site BreachForums Springs Back to Life Weeks After FBI Takedown*, DarkReading (May 29, 2024), available at https://www.darkreading.com/cyberattacks-data-breaches/leak-site-breachforums-springs-back-to-life-weeks-after-fbi-takedown.

the volume of data they acquire and monetize. ShinyHunters often attempts to breach cloud services as a result.[141]

177. For example, in May 2024, ShinyHunters targeted Ticketmaster in a manner that is strikingly similar to the PowerSchool hack, stealing 1.3 terabytes of personal data from Ticketmaster users.[142] "ShinyHunters exploited vulnerabilities in Ticketmaster's cloud storage account with Snowflake to gain access to the information. They hijacked credentials from an employee of a contracting company that worked with Snowflake and used these credentials to infiltrate Snowflake's demo environments. Due to a lack of multifactor authentication, ShinyHunters hackers were able to steal Ticketmaster's data from the cloud storage."[143] The data was then advertised for sale on the dark web[144]:

178. According to Skyhigh Security[145], the typical ShinyHunters modus operandi includes:

> **Orchestrating deception campaigns** by deploying sophisticated phishing schemes that aim to lure victims with fraudulent emails to capture login credentials.
>
> **Targeting unsecured cloud storage** to capitalize on poorly protected online data storage, which is akin to raiding unguarded digital vaults.

---

[141] Obrela Advisory, *ShinyHunters Data Breach Activity Increase* (June 4, 2024), available at https://www.obrela.com/advisory/shinyhunters-data-breach-activity-increase/.

[142] MoneyWatch, *Hacking group claims it breached Ticketmaster and stole data for 560 million customers*, CBS News (updated May 30, 2024), available at https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/.

[143] Romain Basset, *Hard Lessons From the ShinyHunters Data Breaches: Best Practices to CyberSecurity Training*, Training Industry (Aug.1, 2024), available at https://trainingindustry.com/articles/compliance/hard-lessons-from-the-shinyhunters-data-breaches-best-practices-to-cybersecurity-training/.

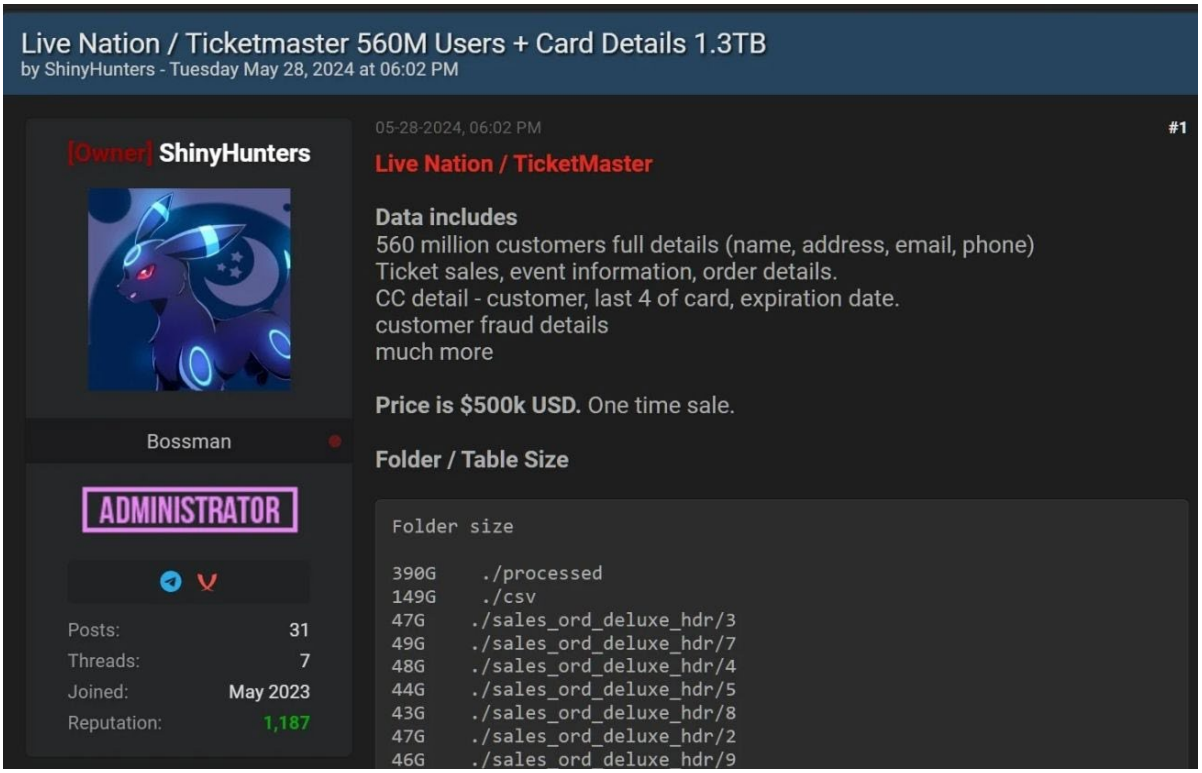
[144] Alina Bizga, *Notorious hacking group claims Ticketmaster data breach*, Bitdefender (May 31, 2024), available at https://www.bitdefender.com/en-gb/blog/hotforsecurity/notorious-hacking-group-claims-ticketmaster-data-breach-personal-details-of-560-million-customers-potentially-compromised/.

[145] Rodman Ramezanian, *Ticketmaster's Encore: How "ShinyHunters" Hacked the Show*, Skyhigh Security (July 11, 2024), available at https://www.skyhighsecurity.com/about/resources/intelligence-digest/ticketmasters-encore-how-shinyhunters-hacked-the-show.html.

Infiltrating and compromising web platforms and development tools, often purloining login details or application programming interface (API) keys to pilfer valuable data.

Probing GitHub repositories to scrutinize company code repositories for exploitable flaws, potentially granting unauthorized database access.

Monetizing via covert networks to profit by trading stolen data on obscure internet marketplaces, catering to buyers seeking illicit information.



179. ShinyHunters also has a history of actually using the data it acquires, not just selling or threatening to sell it. For example, after ShinyHunters hacked Ticketmaster, the group announced that it possessed barcodes for entry to Taylor Swift's Eras tour and "an additional 30 million barcodes for other high-profile concerts and sporting events."[146]

180. ShinyHunters often targets applications with weak API security, including applications that lack multifactor authentication or rate-limiting. By exploiting these weaknesses, they can access sensitive data through exposed API endpoints. Once they

[146] Nick Robins-Early, *Hackers leak alleged Taylor Swift ticket data to extort Ticketmaster*, The Guardian (July 5, 2024), available at https://www.theguardian.com/us-news/article/2024/jul/05/taylor-swift-eras-tour-ticketmaster-hack-ransom.

gain access to an organization's database, ShinyHunters uses APIs to retrieve sensitive data in bulk. This renders organizations that use cloud-hosted databases with inadequate access control, like PowerSchool, likely victims.

181. ShinyHunters is active on the dark web, where the group lists data breaches for sale. It typically offers "exclusive" sales, where only one buyer receives the dataset, or "multi-buy" options, where the dataset is sold to several buyers. The group has carefully cultivated a reputation on forums, which makes buyers more likely to trust and purchase the listings. The group provides "sample" data from breaches to verify authenticity, encouraging purchases by demonstrating the quality of data. ShinyHunters also occasionally "leaks" data in a staged manner to maximize pressure on the victim. The group sometimes releases partial data as a warning, then gives targets a chance to pay before the full release.

182. ShinyHunters has listed data for sale on the dark web even if a ransom is paid. ShinyHunters, for example, hacked AT&T in April 2024, obtaining some 86 million customer records, including customers' SSNs, mailing addresses, and dates of birth.[147] It was reported in July 2024 that AT&T paid ShinyHunters around $370,000 to delete this data.[148] Despite this ransom payment, this data was re-packaged and re-uploaded to a popular Russian cybercrime forum this year.[149]

183. ShinyHunters often begins by searching for companies using Microsoft Office 365 and third parties that store GitHub open authorizations tokens.[150] The group

---

[147] Christianna Silva, *Hackers leak 86 million AT&T customer records with 44 million social security numbers, report says*, Mashable (June 6, 2025), available at https://mashable.com/article/leaked-att-customer-record-social-security-numbers.

[148] Kim Zetter, *AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records,* WIRED (July 14, 2024), available at https://www.wired.com/story/atandt-paid-hacker-300000-to-delete-stolen-call-records/.

[149] Chris Riotta, *AT&T Hit by Massive Reported Identity Data Leak – Again*, Bank Info Security (June 5, 2025), available at https://www.bankinfosecurity.com/att-hit-by-massive-reported-identity-data-leak-again-a-28595.

[150] *Researchers Share Common Tactics of ShinHunters Threat Group*, DarkReading (Aug. 24, 2021) available at https://www.darkreading.com/cyberattacks-data-breaches/researchers-share-common-tactics-of-shinyhunters-threat-group.

then identifies research, development, and other employees with broad access to data in the organizations. ShinyHunters also has a history of attacking developer repositories to steal credentials or API keys.[151] The following graphic summarizes ShinyHunters tactics[152]:

[151] Ravie Lakshmanan, *Researchers Detail Modus Operandi of ShinyHunters Cyber Crime Group*, The Hacker News (Aug. 23, 2021), available at https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html.

[152] *Here's how to guard your enterprise against ShinyHunters*, Intel471 (Aug. 23, 2021), available at https://intel471.com/blog/shinyhunters-data-breach-mitre-attack. The TA0043 Reconnaissance refers to the MITRE groups description of reconnaissance techniques. Mitre Attack, *Reconnaissance*, https://attack.mitre.org/tactics/TA0043/ (last visited July 23, 2025).

ShinyHunters Scenario Most Likely Courses of Action	ShinyHunters Scenario Most Dangerous Courses of Action
RECONNAISSANCE [TA0043]	
Identify organizations using Microsoft Office 365 and search for valid accounts.	Identify third-party companies that store GitHub open authorization (OAuth) tokens. Identify and research development and operations (devops) personnel.
WEAPONIZATION	
Identify credentials for valid accounts from leaked and/or previously stolen credential data sets. Purchase credentials on marketplaces such as Genesis. Use accounts to log in to cloud services.	Hack third-party companies to steal OAuth tokens, leverage them to bypass two-factor authentication (2FA) and gain access to cloud services. Directly target devops personnel to phish valid GitHub repository credentials.
DELIVERY [TA0001]	
Directly target database vulnerabilities to access sensitive information.	Target software repositories to access application programming interface (API) keys, OAuth keys, hard-coded credentials and more.
EXPLOITATION	
Steal sensitive data such as credentials and PII. Exploit remote service tools.	Audit source code to find vulnerabilities that can be leveraged in larger scale attacks.
COMMAND AND CONTROL [TA0011]	
Exfiltrate data via web services. Alternate domain name system (DNS) records to redirect legitimate traffic. Use exploited nodes as a vector and/or exit node for future attacks.	Leverage legitimate credentials and tools such as GitHub utilizing OAuth which makes it more difficult to detect.
ACTIONS ON OBJECTIVES [TA0040]	
Sell stolen data on forums for profit.	Extort, blackmail and expose information in the underground.
OUTCOME	
Confidentiality: Information theft and espionage. Integrity: Modification or deletion of data from an unauthorized party. Availability: Unable to update or access the environment until it is secured and accounts are reset.	Confidentiality: Private information available publicly. Integrity: Modification or deletion of data from an unauthorized party. Availability: Unable to update or access the environment until it is secured and accounts are reset.

INTEL471

184. In sum, ShinyHunters is a notorious, decentralized hacking group whose tactics are well-known and foreseeable. Indeed, the substantially similar Ticketmaster hack happened mere months before the Data Breach here. Because PowerSchool maintained a massive cloud-based userbase of teachers and students, it was a predictable target. Making PowerSchool even more tempting, it did not employ multifactor authentication or other basic security measures for contractors who had access to vast troves of data belonging to millions. Nonetheless, as explained more fully below, PowerSchool failed to take even basic steps to protect against this foreseeable risk.

N. DEFENDANTS FAILED TO TAKE NECESSARY OR REASONABLE STEPS TO SAFEGUARD PII

185. Defendants failed to implement basic data security measures that are common across the industry and recommended by the National Institute of Standards and Technology ("NIST"),[153] the Cybersecurity and Infrastructure Security Agency ("CISA"),[154] the System and Organization Controls 2 ("SOC 2"), and countless other agencies and industry experts.[155] Worse yet, PowerSchool itself recommended many

[153] NIST is a component agency of the United States Department of Commerce that has developed a voluntary framework—based on existing standards, guidelines, and practices— for reducing cyber risks to critical infrastructure. Created through collaboration between industry and government, the voluntary framework promotes the protection of critical infrastructure, and provides standards, guidelines, tools, and technologies to protect information technology systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services. *See* NIST, *Cybersecurity*, https://www.nist.gov/cybersecurity.

[154] CISA is a component agency of the United States Department of Homeland Security. CISA develops guidelines to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, resilience of national critical functions, and a robust technology ecosystem. *See* CISA, *Cybersecurity Division*, available at https://www.cisa.gov/about/divisions-offices/cybersecurity-division.

[155] SOC 2 is a framework that includes criteria and guidance developed by the American Institute of Certified Public Accountants (AICPA). for service organizations to manage and report on their security, availability, processing integrity, confidentiality, and privacy of customer data. *See, e.g.*, AICPA & CIMA, 2018 SOC 2® Description Criteria (With Revised Implementation Guidance – 2022),

Footnote continued on next page

of these measures as best practices, but failed to heed its own advice.[156] Specifically, contrary to industry standards and, in many instances, its own recommendations, PowerSchool failed to: (1) implement multifactor authentication (2) implement the principle of least privileges, (3) implement the principle of network segmentation, (4) implement rate limiting, (5) secure the contractor's credentials, (6) monitor its logs for unusual activity, (7) adequately implement an intrusion detection and prevention system, (8) permanently delete unnecessary PII, and (9) encrypt the data. Likewise, while the full scope of Movate's failures will be revealed in discovery, Movate also failed to (1) appropriately train its employees to secure their credentials; (2) rotate its employees' credentials; (3) and implement the principle of least privileges.

1. POWERSCHOOL FAILED TO IMPLEMENT MULTIFACTOR AUTHENTICATION.

186. Multifactor authentication is "a simple way to protect [an] organization and can prevent a significant number of account compromise attacks."[157] It is an "important security enhancement that requires a user to verify their identity by providing more than just a username and password."[158]

https://www.aicpa-cima.com/resources/download/get-description-criteria-for-your-organizations-soc-2-r-report.

[156] *See, e.g.*, PowerSchool, Top 6 Best Practices for Improving Student Information System (SIS) Cybersecurity (Sept. 10, 2024), https://www.powerschool.com/blog/best-practices-improving-sis-cybersecurity/.

[157] CISA, *Require Multifactor Authentication*, https://www.cisa.gov/secure-our-world/require-multifactor-authentication (last visited July 23, 2025).

[158] NIST, *Multi-Factor Authentication*, https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication (last visited July 23, 2025).

187. Multifactor authentication has been industry standard for more than a decade.[159,160,161,162] The 2014 book *CompTIA Security+ Review Guide: Exam SY0-4*01 strongly recommends two-factor authentication.[163] The 2012 book *Hacking Exposed 7: Network Security Secrets and Solutions* also strongly recommends two-factor authentication.[164]

188. Not using multifactor authentication is a substantial breach of standard data security practices. The Federal Bureau of Investigation,[165] Department of Education,[166] National Institute of Standards and Technology,[167] multiple educational

[159] Rose de Fremery, *The Evolution of Multi-Factor Authentication*, LastPass (Dec. 22, 2021), available at https://blog.lastpass.com/posts/the-evolution-of-multi-factor-authentication.

[160] *History of Authentication: From Zero to Hero*, Asee (June 7, 2022), available at https://cybersecurity.asee.io/blog/history-of-authentication/.

[161] *The History of MFA/Multi-Factor Authentication*, University of Wisconsin-Madison, https://law.wisc.edu/news/Law_Library/The_History_of_MFA_Multi_Factor_2024-09-17 (last visited July 23, 2025).

[162] *Multifactor Authentication Cheat* Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html (last visited July 23, 2025).

[163] Stewart, James M., CompTIA Security+ Review Guide: Exam SY0-401. Wiley.

[164] McClure, Stuart. Hacking Exposed 7: Network Security Secrets and Solutions. McGraw Hill LLC. Kindle Edition.

[165] FBI, *Ransomware Victims Urged to Report Infections to Federal Law Enforcement* (Sept. 15, 2016), available at https://www.ic3.gov/PSA/2016/psa160915.

[166] *K-12 Cybersecurity*, U.S. Dept. of Ed., https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity (last visited July 23, 2025).

[167] NIST, *supra* n.109.

organizations, [168,169,170,171,172] the CyberSecurity & Infrastructure Security Agency,[173] and countless other agencies and organizations[174] strongly recommend multifactor authentication. It is also covered on standard cybersecurity certification examinations, including the CompTIA Security+ examination[175] and the ISC2 Certified Information System Security Professional (CISSP) examination.[176]

---

[168] April Mardock, *Why Multifactor Authentication Should No Longer Be Optional in K-12*, EdTech (June 28, 2024), available at https://edtechmagazine.com/k12/article/2022/03/why-multifactor-authentication-should-no-longer-be-optional-k-12.

[169] *Microsoft Multi-Factor Authentication*, Univ. of Alabama, https://oit.ua.edu/software/duo/duo-faqs/microsoft-multi-factor-authentication/ (last visited July 23, 2025).

[170] *Multi-factor Authentication at Northwestern*, Northwestern, https://services.northwestern.edu/TDClient/30/Portal/KB/ArticleDet?ID=1901 (last visited July 23, 2025).

[171] *Microsoft multi-factor authentication*, Purdue Univ., https://it.purdue.edu/mfa/ (last visited July 23, 2025).

[172] Corinne Boyer, *Why You Should BE Using Multifactor Authentication For your Online Accounts*, Univ. of Ky. (Oct. 24, 2024), available at https://its.uky.edu/news/why-you-should-be-using-multifactor-authentication-all-your-online-accounts.

[173] CISA, *supra* n.108. The same is true of the Payment Card Industry Data Security Standards. *See, e.g.*, https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf.

[174] *What is a single sign-on*, Citrix, https://www.citrix.com/glossary/what-is-single-signon-sso.html (last visited Dec. 3, 2024); *Multi-factor authentication: Key protection to tax professionals' security arsenal now required*, IRS (Aug. 6, 2024), https://www.irs.gov/newsroom/multi-factor-authentication-key-protection-to-taxprofessionals-security-arsenal-now-required; *Multi-Factor Authentication*, PCI SECURITY STANDARDS COUNCIL (Feb. 2017), https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-25_v1.pdf; *A guide to the FTC Safeguards Rule's FTC MFA requirement*, IS DECISIONS (July 21, 2023), https://www.isdecisions.com/en/blog/compliance/compliance-with-the-ftcmfa-requirement; *PCI DSS 4.0: New multi-factor authentication requirements*, ONESPAN (May 23, 2024), https://www.onespan.com/blog/new-mfa-requirements-in-PCI-DSS-4.0; *Multifactor Authentication Cheat Sheet*, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet .html (last visited Jun. 18, 2025).

[175] *CompTIA Security+ Certification Exam Objectives*, CompTIA (2023), available at https://lecbyo.files.cmp.optimizely.com/download/cf25ec24b8a511ef9ecbb69c0f9687be.

[176] *CISSP Certification Exam Outline Summary*, ISC2, https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline (last visited July 23, 2025).

189. Microsoft and Google reported in 2019 that using multifactor authentication blocks more than 99% of automated hacks, including most ransomware attacks resulting from unauthorized account access.[177]

190. In fact, PowerSchool itself has repeatedly recommended multifactor authentication. For example, PowerSchool's Vice President of Cyber Threat Management recognized in a YouTube video that multifactor authentication is an "essential tool" and "must-have feature" for school districts.[178] It "enhances security significantly because criminals can't just guess your password" to access troves of data.[179]

191. Likewise, in another YouTube video uploaded on September 25, 2023, titled "5 Ways PowerSchool Helps Secure Your District," PowerSchool notes that "PowerSchool offers free single sign-on or multifactor authentication support" in its bundle of services.[180]

192. In an article that appears to have been deleted shortly after the Data Breach, PowerSchool recognized that "[i]mplementing Single Sign-On (SSO) and Multi-Factor Authentication (MFA) is a best practice that significantly boosts your school's cybersecurity" because it "ensures that even if a password is compromised, unauthorized access is still prevented."[181] A graphic outlined multifactor authentication

---

[177] *How effective is multifactor authentication at deterring cyberattacks?*, Microsoft, available at https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MFA-Microsoft-Research-Paper-update.pdf?culture=en-ca&country=ca (last visited July 21, 2025).

[178] PowerSchool, *What Is Multi-Factor Authentication*, https://www.youtube.com/watch?v=_rQ4qCY1rpc (last visited July 17, 2025).

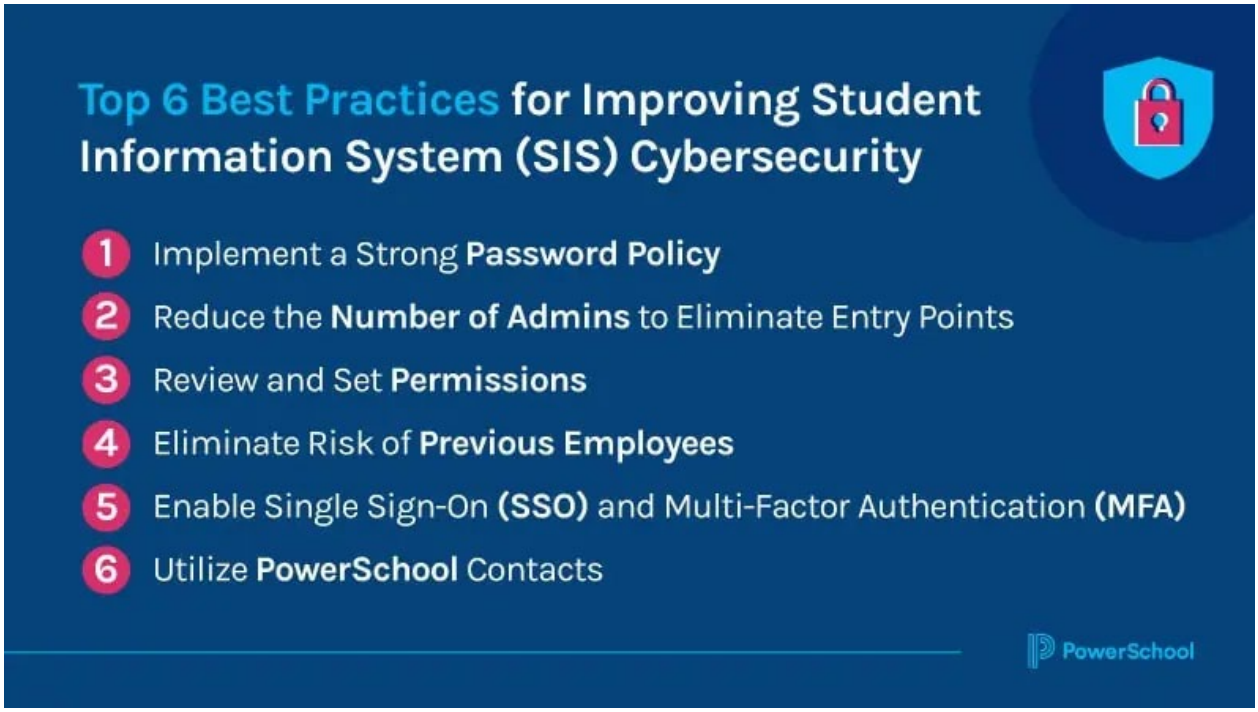
[179] *Id.*

[180] PowerSchool, *5 Ways PowerSchool Helps Secure Your District*, https://www.youtube.com/watch?v=vRJOR5iEaS8 (last visited July 17, 2025).

[181] Internet Archive, *PowerSchool: Top 6 Best Practices for Improving Student Information System (SIS) Cybersecurity*, https://web.archive.org/web/20241215031755/https://www.powerschool.com/blog/best-practices-improving-sis-cybersecurity/ (last visited July 17, 2025).

among six best practices (some of which are also described below) to protect student and teacher data:[182]

193. By failing to implement one of the most basic and universally recommended best practices for the Movate employee who had access to all of PowerSchool's data on teachers and families, PowerSchool failed to comply with industry standards and its own advice.[183] Had the Movate employee account required multifactor authentication, the Data Breach would not have happened because a simple username and password would have been insufficient for ShinyHunters to gain access.



2. POWERSCHOOL AND MOVATE FAILED TO IMPLEMENT THE PRINCIPLE OF LEAST PRIVILEGES.

194. One of the most fundamental principles of cybersecurity is the principle of least privileges. Every account should have only enough access privileges to conduct

[182] *Id.*

[183] Kevin Collier, *Children's data hacked after school software firm missed basic security step, internal report says*, NBC News (Jan. 31, 2025), available at https://www.nbcnews.com/tech/security/powerschool-hack-data-breach-protect-student-school-teacher-safe-rcna189029.

required job functions and no more.[184] This has been a principle of cybersecurity for decades: no single account should be able to access all data.[185,186,187,188,189]

195. This principle is incorporated in the 2008 NIST Special Publication 800-123 Guide to General Server Security.[190] CISA guidance further recommends use of the principle of least privilege should be applied to all systems so that users only have the access they need to perform their jobs.[191] SOC 2 likewise recognizes and recommends the concept of least privileges.[192] The FBI also recommends that "no users should be assigned administrative access unless absolutely needed."[193] It is also covered on standard cybersecurity certification examinations, including the CompTIA

---

[184] Pascal Meunier, *Confusion of Separation of Privilege and Least Privilege*, The Center for Education and Research in Information Assurance and Security (Jan. 15, 2008), available at https://www.cerias.purdue.edu/site/blog/post/confusion-of-separation-of-privilege-and-least-privilege/.

[185] Fred B. Schneider, *Least Privilege and More*, Cornell University, available at https://www.cs.cornell.edu/fbs/publications/leastPrivNeedham.pdf.

[186] *Understanding Core Security Principles*, Wiley, available at https://catalogimages.wiley.com/images/db/pdf/9781118016848.c01.pdf.

[187] *An Overview of Computer Security*, Pearson, available at https://www.pearsonhighered.com/assets/samplechapter/0/2/0/1/0201440997.pdf.

[188] Steven M. Bellovin, *Acquiring Privileges*, Columbia University Computer Science Department (Jan. 24, 2007), available at https://www.cs.columbia.edu/~smb/classes/s07/l04.pdf.

[189] Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne, *Protection*, Operating System Concepts Essentials – 8th Edition (2011), available at: https://codex.cs.yale.edu/avi/os-book/OS8/os8e/slide-dir/PDF-dir/ch13.pdf.

[190] Karen Scarfone, Wayne Jansen, and Miles Tracy, *Guide to General Server Security*, National Institute of Standards and Technology (July 2008), available at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf.

[191] *Ransomware Guide*, Multi-State Information Sharing & Analysis Center, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security, at 4 (Sept. 2020), available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

[192] *2018 SOC 2® Description Criteria (With Revised Implementation Guidance – 2022)*, AICPA & CIMA (Oct. 1, 2023) § CC 6.1, 6.3, available at https://www.aicpa-cima.com/resources/download/get-description-criteria-for-your-organizations-soc-2-r-report.

[193] FBI, *Ransomware Prevention and Response for CISOs*, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

Security+ examination[194] and the ISC2 Certified Information System Security Professional (CISSP) examination.[195]

196. PowerSchool itself recommended the principle of least privileges as a best practice in a September 10, 2024 article posted on its website.[196] PowerSchool recognized the problem that, too often, "too many individuals have administrative access to critical systems" and that "[t]he principle of least privilege should be applied, meaning users should have the minimum level of access necessary to perform their job functions."[197]

197. However, the Movate employee whose credentials were compromised and used in carrying out the Breach apparently had access to *all* student and teacher data housed by PowerSchool. This individual had no need for unfettered access to so much data, much less for access that allowed exfiltration. Had PowerSchool and Movate effectively implemented the principle of least privileges, the Movate employee would have never been able to access, much less exfiltrate, the Data, and ShinyHunters would not have been able to access sensitive information for every Plaintiff and Class Member.

3. POWERSCHOOL FAILED TO IMPLEMENT THE PRINCIPLE OF NETWORK SEGMENTATION.

198. A related but distinct principle to least privileges is the principle of network segmentation. "Network segmentation permits unrelated portions of the

[194] *CompTIA Security+ Certification Exam Objectives*, CompTIA, (2023), available at https://lecbyo.files.cmp.optimizely.com/download/cf25ec24b8a511ef9ecbb69c0f9687be.

[195] *CISSP Certification Exam Outline Summary*, ISC2, (Apr. 15, 2024), available at https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline.

[196] *Top 6 Best Practices for Improving Student Information System (SIS) Cybersecurity*, PowerSchool (Sept. 10, 2024), available at https://www.powerschool.com/blog/best-practices-improving-sis-cybersecurity/.

[197] *Id.*

entity's information system to be isolated from each other."[198] If this principle is implemented and cyberthreat actors target one segment of data, the attack can be contained to that segment instead of all data.[199]

199. CISA,[200] NIST,[201] and SOC 2[202] all recommend network segmentation.

200. Network segmentation can be implemented in either on-premises, physical networks or in cloud-based networks like PowerSchool's SIS. Virtual Local Area Network are one common way to segregate data on cloud-based networks.[203]

201. ShinyHunters was able to exfiltrate massive tables of student and teacher data that contained contact information, grades, medical information, and numerous other categories of sensitive data outlined above. If PowerSchool had implemented network segmentation, ShinyHunters would have only been able to access some of Plaintiffs' and Class Members' data instead of the wide-ranging Data subject to the Data Breach.

4. POWERSCHOOL FAILED TO IMPLEMENT RATE LIMITING.

202. Rate limiting is a technique used to control the amount of incoming or outgoing traffic to or from a system, service, or application. Its primary purpose is to

---

[198] SOC 2, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (updated March 2020), available at https://assets.ctfassets.net/rb9cdnjh59cm/72xv4p67HVXKp6CjWmjkPk/1cdbfa19f6307e2720396b66a6194dc9/trust-services-criteria-updated-copyright.pdf.

[199] https://insights.sei.cmu.edu/blog/network-segmentation-concepts-and-practices/.

[200] CISA, *Layering Network Security Through Segmentation Infographic*, https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic (last accessed July 17, 2025).

[201] NIST SP 800-215, available at https://csrc.nist.gov/pubs/sp/800/215/final; NIST SP 800-125B.

[202] 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (updated March 2020), available at https://assets.ctfassets.net/rb9cdnjh59cm/72xv4p67HVXKp6CjWmjkPk/1cdbfa19f6307e2720396b66a6194dc9/trust-services-criteria-updated-copyright.pdf.

[203] https://dev-rhevm.ldeo.columbia.edu/ovirt-engine/docs/Technical_Reference/Virtual_LAN_VLAN.html; *CAS Login*, Dept. of Computer Science Computing Guide, https://csguide.cs.princeton.edu/access/vlans (last visited July 23, 2025).

ensure stability, availability, and fair use of system resources, and to protect against abuse or denial-of-service (DoS) attacks. Rate limiting restricts the number of actions a user, IP address, or client can perform within a specific time frame.[204,205]

203. Had PowerSchool appropriately configured rate limiting, ShinyHunters would have been limited in how much data it could download. The Breach could have been slowed and, in combination with other common data security measures PowerSchool failed to take, stopped before the Data was exfiltrated.

5. POWERSCHOOL AND MOVATE FAILED TO ADEQUATELY SECURE CREDENTIALS.

204. Most online credentials are rotated on a regular basis so that, if a threat actor obtains a user's credentials, there is only a short window of time that the threat actor can exploit a data security vulnerability. Through this mitigation effort, "authentication credentials, such as passwords, API keys, or certificates, are regularly changed or replaced to minimize the risk of unauthorized access."[206]

205. Not everyone's credentials within an organization need to be changed frequently. However, individuals with "superuser accounts and other privileged end-user credentials will likely need more frequent rotation" even more frequent than every 60 or 90 days.[207]

206. In addition, CISA recommends other steps to secure credentials, including requiring strong, unique passwords, providing an enterprise-level password manager,

---

[204] Barath Raghavan, et al., *Cloud Control with Distributed Rate Limiting*, Univ. of Calif. (2007), https://raghavan.usc.edu/papers/drl-sigcomm07.pdf.

[205] M. Bowden, et al., *Rate Limiting in Linux* (June 30, 2006), available at https://people.computing.clemson.edu/~jmarty/courses/LinuxStuff/LinuxRateLimit.pdf.

[206] MITRE, *D3-CRO*, available at https://d3fend.mitre.org/technique/d3f:CredentialRotation/ (last visited July 1, 2025).

[207] SSH Academy, *Password and Key Rotation*, available at https://www.ssh.com/academy/secrets-management/password-key-rotation#:~:text=Some%20credentials%2C%20such%20as%20passwords,too%20often%20than%20too%20little. (last visited July 17, 2025).

and requiring that default credentials be changed on all software and hardware products.[208]

207. PowerSchool and Movate failed to take reasonable steps to prevent Mr. Cruz's credentials from being compromised, including by failing to properly train their employees, and by failing to properly detect and block phishing attempts and to secure open ports.[209]

208. In particular, PowerSchool and Movate could have prevented the Breach by rotating the credentials of Movate employees on a regular basis. If PowerSchool or Movate had a policy of changing high-value credentials every 90 days, for example, credentials that enabled access in August 2024 would have been stale by the time ShinyHunters started exfiltrating data in December 2024. In other words, had PowerSchool or Movate adequately rotated credentials of Movate employees working on the PowerSchool account, the Data Breach would not have happened.

6. POWERSCHOOL FAILED TO MONITOR ITS LOGS FOR UNUSUAL ACTIVITY.

209. Log monitoring involves the continuous analysis of system, application, and device logs to detect unusual activity. It is critical for maintaining system health, security, and performance. It enables timely detection of issues, efficient troubleshooting, and proactive threat mitigation. By analyzing logs, organizations can gain insights into system behavior, user activity, and potential security breaches, ultimately enhancing overall system resilience.

---

[208] CISA, *Require Strong Passwords*, available at https://www.cisa.gov/secure-our-world/require-strong-passwords (last visited July 29, 2025); *see also* CISA, *Cybersecurity Advisory: Weak Security Controls and Practices Routinely Exploited for Initial Access*, available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a (last visited July 29, 2025).

[209] CISA, Cybersecurity Advisory: Weak Security Controls and Practices Routinely Exploited for Initial Access, available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a (last visited July 29, 2025).

210. Log monitoring is important because, "to expose an attack or identify the damage caused, you need to analyze the log events on your network in real-time. By collecting and analyzing logs, you can understand what transpires within your network. Each log file contains many pieces of information that can be invaluable, especially if you know how to read them and analyze them. With proper analysis of this actionable data you can identify intrusion attempts, mis-configured equipment, and many more."[210] The Payment Card Industry Data Security Standard (PCI-DSS) also requires log monitoring.[211,212]

211. The National Institute of Standards and Technology 2006 standard NIST SP 800-9 Guide to Computer Security Log Management[213] provides detailed recommendations on log management, including log monitoring. Likewise, CISA and a dozen cybersecurity agencies across the world recognize that log monitoring "improves an organisation's chances of detecting malicious behaviour on their systems and enforces a consistent method of logging across an organisation's environments."[214] The Center for Internet Security lists "Audit Log Management" as one of its 18 "Critical Security Controls."[215]

---

[210] Wang Wei, *Importance of Logs and Log Management for IT Security*, The Hacker News (Oct. 2, 2013), available at https://thehackernews.com/2013/10/importance-of-logs-and-log-management.html.

[211] George Mateaki, *PCI Requirement 10: Logging and Log Monitoring*, Security Metrics, https://www.securitymetrics.com/blog/pci-requirement-10-logging-and-log-monitoring (last visited July 23, 2025).

[212] *Effective Daily Log Monitoring*, PCI Security Standard Council (May 2016), https://listings.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf.

[213] Karen Kent, et al., *Guide to Computer Security Log Management*, NIST https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf (last visited July 23, 2025).

[214] Australian Signals Directorate's Australian Cyber Security Centre et al., *Best practices for event logging and threat detection*, available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-234a.

[215] Center for Internet Security, *The 18 CIS Critical Security Controls*, https://www.cisecurity.org/controls/cis-controls-list (last visited July 17, 2025). The Payment Card Industry Data Security Standard (PCI-DSS) also requires log-monitoring. *See, e.g.,* https://listings.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf.

212. All of the available information indicates that PowerSchool failed to monitor its logs. According to the CrowdStrike Report, the timeline of events is as follows:

Date/Time	***Activity***
8/16/2024 01:27:29 UTC	Beginning of unknown actor access
9/17/2024	End of unknown actor access
12/19/2024 04:06:24 UTC	First activity attributable to the Threat Actor
12/19/2024 23:02:54 UTC	Beginning of Data exfiltration
12/23/2024 08:04:45 UTC	End of Data exfiltration
12/28/202404:06:24 UTC	PowerSchool is alerted to suspicious activity

213. In other words, PowerSchool did not notice suspicious activity until five days after data exfiltration ended, nine days after it began, and over *four months* after logs show an unknown actor was already accessing PowerSchool's systems. Moreover, the data exfiltration took four days to accomplish, but PowerSchool failed to have logging in place to detect this massive export of data from its systems.

214. PowerSchool's logs did not go back far enough to determine if any other malicious activity had taken place, because CrowdStrike was unable to verify whether the August intrusions came from the same IP address as that used in the Data Breach.

215. This timeline demonstrates that there were unknown individuals accessing PowerSchool at least four months prior to PowerSchool noticing any activities. The fact that at least some of these intrusions took place from a VPN using a server in Ukraine is even more alarming. Any adequate system would have recognized that a computer in Ukraine accessing the entirety of PowerSchool's systems through the Philippines was a massive red flag.

216. This timeline also demonstrates that PowerSchool had no system in place to monitor the exfiltration of large amounts of data. Even after failing to recognize

unusual user access, PowerSchool still might have prevented the Data Breach if its systems were capable of recognizing unusual exfiltration activity on December 19, 2024. The exfiltration took four days, and PowerSchool had no system in place to recognize and stop what was happening as it was happening between December 19 and 23, 2024.

217. If PowerSchool had adequately implemented log monitoring, this unusual activity would have been detected, and ShinyHunters would not have been able to successfully access and exfiltrate the Data.

7. POWERSCHOOL FAILED TO IMPLEMENT AN INTRUSION DETECTION AND PREVENTION SYSTEM.

218. An intrusion detection system is a security solution that monitors network traffic or system activities for suspicious behavior and known threats, issuing alerts when potential intrusions are detected.[216,217] An intrusion prevention system is a more active counterpart to an intrusion detection system. It not only detects threats but also automatically takes action to prevent or block malicious activity in real time.[218]

219. NIST recognizes that "intrusion detection systems have become a necessary addition to the security infrastructure of most organizations."[219] Being able to flag intrusions early is important because "[t]he first stage of an attack is usually probing or examining a system or network, searching for an optimal point of entry."[220] A properly functioning system "will identify them as suspicious, may actively block the attacker's access to the target system, and will alert security personnel who can then

---

[216] *Intrusion Detection*, John Hopkins, Course Description, https://ep.jhu.edu/courses/695642-intrusion-detection/ (last visited July 23, 2025).

[217] *Intrusion Detection Guideline*, UC Berkeley, https://security.berkeley.edu/intrusion-detection-guideline (last visited July 23, 2025).

[218] Ed Sale, *Intrusion Detection and Intrusion Prevention*, Pivot Group, https://www.cs.unh.edu/~it666/reading_list/Defense/ids_vs_idp.pdf (last visited July 23, 2025).

[219] Rebecca Bace and Peter Mell, *NIST Special Publication on Intrusion Detection Systems*, NIST (Nov. 1, 2001).

[220] *Id.* § 2.2.3.

take appropriate actions to block subsequent access by the attacker."[221] NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)[222] provides guidance on how to configure these systems and why an organization should have them.

220. Likewise, the FBI, CISA, and the NSA recommend "leveraging intrusion detection system/intrusion prevention system sensors to detect anomalous network activity."[223]

221. If PowerSchool employed an adequate intrusion detection and prevention system, ShinyHunters' attempts to access the Movate employee's account in August 2024 would have stopped there and then. In December 2024, any adequate system would have also detected—and stopped—unusual activity, including logging in from an unusual IP address, accessing data not previously accessed, and downloading large volumes of data.

8. POWERSCHOOL FAILED TO PERMANENTLY DELETE UNNECESSARY DATA.

222. PowerSchool failed to permanently delete unnecessary data.

223. The cybersecurity principle that governs the deletion of unnecessary data is called Data Minimization.

224. This principle dictates that organizations should only collect, process, and store data that is strictly necessary for defined objectives. It emphasizes that retaining data beyond its useful life or business value introduces unnecessary costs and risks, including increased vulnerability to data security incidents, like breaches.

225. Data minimization assures that companies responsibly dispose of data once its intended purpose has been fulfilled. This practice significantly reduces the

---

[221] *Id.*

[222] Karen Scarfone, Peter Mell, *Guide to Intrusion Detection and Prevention Systems*, NIST (February 2007), https://csrc.nist.gov/pubs/sp/800/94/final.

[223] CISA, *Weak Security Controls and Practices Routinely Exploited for Initial Access* (Dec. 8, 2022), available at https://www.cisa.gov/news-events/alerts/2022/05/17/weak-security-controls-and-practices-routinely-exploited-initial-access.

volume of data that could be compromised in a data breach, thereby lessening the potential impact and consequences.

226. PowerSchool failed to implement data minimization and kept data for students who had graduated and whose information was no longer necessary in the SIS system.

9. POWERSCHOOL FAILED TO ENCRYPT ITS DATA.

227. Cloud encryption is a data security best practice by which data is transformed "from its original plain text format to an unreadable format, such as ciphertext, before it is transferred to and stored in the cloud."[224] Data can be encrypted while being transferred between databases or it can be encrypted "at rest."[225] This practice "ensures that even if the data is lost, stolen or mistakenly shared, the contents are virtually useless without [an] encryption key."[226]

228. The Center for Internet Security emphasizes that "[t]he adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise and, more importantly, is a regulatory requirement for most controlled data."[227] Likewise, the NSA and CISA recognize that "[e]ncryption at rest and in transit is an imperative for sensitive data."[228]

229. AES (Advanced Encryption Standard) is one widely-used cryptography algorithm by which organizations can encrypt their data. But even if an organization uses AES, it is worthless unless adequately implemented. For example, if a single key

---

[224] Cody Queen, *Cloud Encryption Explained*, CrowdStrike (Mar. 5, 2025), available at https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-encryption/.

[225] *Id.*

[226] *Id.*

[227] *CIS Control 3: Data Protection*, available at https://cas.docs.cisecurity.org/en/latest/source/Controls3/ (last visited July 23, 2025).

[228] NSA and CISA, *Secure Data in the Cloud* (March 2024), available at https://media.defense.gov/2024/Mar/07/2003407862/-1/-1/0/CSI-CLOUDTOP10-SECURE-DATA.PDF.

from a single individual could access and decrypt all Data upon logging in, AES encryption would serve no purpose.

230. If the Data had been adequately encrypted, ShinyHunters may have technically been able to download the Data—sensitive data belonging to tens of millions of people—but it would have been unreadable and therefore useless.

O. COMPROMISED DATA PRESENTS SERIOUS RISK OF IDENTITY THEFT

231. Identity theft is the "natural next step that follows a breach."[229] "Data breaches commonly lead to identity theft and identity fraud because malicious actors can gain easy access to large amounts of data, including names, addresses, dates of birth, and Social Security Numbers."[230]

232. Identity theft is a serious, expensive, and time-consuming problem. In 2023, identity fraud affected 15 million Americans, costing an estimated $43 billion.[231] In that same year, a victim of identity theft spent an average of nearly 10 hours attempting to resolve the fraud.[232]A family will spend even more time—an estimated 13 to 16 hours—resolving identity theft involving a minor.[233] Victims of identity theft may also experience damage to their credit scores and criminal records, as well as a myriad of other consequences.

---

[229] *Data Breaches and Data Theft*, UCLA, https://ociso.ucla.edu/cybersecurity-you/protect-your-identity (last visited July 23, 2025).

[230] Matt Galardi, *The Hidden Costs of a Data Breach*, Univ. of Neb., https://www.unomaha.edu/news/2016/02/february-information-security-newsletter-the-hidden-costs-of-a-data-breach.php (last visited July 23, 2025).

[231] Christina Ianzito, *Identity Fraud Cost Americans $43 Billion in 2023*, AARP (April 10, 2024), available at https://www.aarp.org/money/scams-fraud/identity-fraud-report-2024/.

[232] Suzane Sando, *2024 Identity Fraud Study: Resolving the Shattered Identity Crisis*, Javelin (April 10, 2024), available at https://javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis.

[233] *Child Identity Fraud*, Javelin (Oct. 2022), https://javelinstrategy.com/sites/default/files/files/reports/22-5012J-FM-2022%20Child%20Identity%20Fraud%20Study.pdf at 12.

233. Identity theft can have devastating emotional and physical impacts, too. According to a study by the Identity Theft Resource Center, 86% of victims of identity theft reported feeling worried, angry, and frustrated; almost 70% felt they could not trust others and that they felt unsafe; 59% reported feeling sadness or depression; and half reported losing interest in activities or hobbies that they once enjoyed.[234] Worse yet, a 2023 survey found that 16% of identity fraud victims had contemplated suicide, compared to just 5% of the general population.[235]

234. Victims of identity theft can also experience physical repercussions. For example, in the Identity Theft Resource Center study, nearly 85% of identity theft victims reported disturbances in their sleep habits; 77% reported increased stress levels; nearly 64% said they had trouble concentrating; and nearly 57% reported having aches, pains, headaches, and cramps.[236]

1. CRIMINALS, INCLUDING THIEVES LIKE SHINYHUNTERS, CAN USE PII TO COMMIT IDENTITY FRAUD

235. There are countless ways that criminals can use PII to wreak havoc on the individuals whose information has been breached. This is true of the criminals that initially obtain the stolen data—here, ShinyHunters—as well as any criminals who later get their hands on the data.

236. As CrowdStrike has explained: "Traditionally, identity theft involves the appropriation and misuse of an existing person's identity."[237] In other words, a

---

[234] Jessica Guynn, *Anxiety, depression and PTSD: The hidden epidemic of data breaches and cyber crimes*, USA Today (updated Feb. 24, 2020), available at https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/.

[235] *2023 Consumer Impact Report*, Identity Theft Resource Center (Aug. 2023) at 6, available at https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.

[236] Guynn, *supra* n.184.

[237] Ryan Terry, *Synthetic Identity Fraud Explained*, CrowdStrike (March 10, 2025), available at https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/synthetic-identity-fraud/.

cybercriminal uses all of the victim's personal and *real* information—for example, SSN, driver's license number, credit card number, and telephone number—without the victim's permission.[238]

237. However, cybercriminals have become more sophisticated over time, and can now use a single piece of an individual's PII—for example, their home address or SSN—to perpetrate identity theft. Ultimately, what criminals can do depends on the data that they have.

a. ANY PII CAN BE USED TO COMMIT FRAUD

238. As a preliminary matter, effectively *any* piece of PII stolen in a data breach can be used to commit identity fraud. There are two primary ways that cybercriminals can use a single piece of seemingly innocuous PII to carry out identity theft.

b. SYNTHETIC IDENTITY FRAUD

239. Unlike traditional identity theft—where a fraudster poses as their victim—synthetic identity fraud "involves constructing a fabricated identity that is a mash-up of both authentic and fabricated details."[239] Thus, "[t]he resulting identity appears legitimate on paper but does not represent an actual person."[240]

240. "For example, a synthetic identity may be created by stealing a real SSN and combining it with a false name, date of birth and address. This new, fake identity is then used to commit acts of fraud."[241] "These 'Frankenstein IDs' may appear legitimate on the surface, allowing criminals to open new accounts, obtain credit cards, and even secure loans."[242]

---

[238] *Identity Theft*, Harvard Univ., https://www.hupd.harvard.edu/identity-theft (last visited July 23, 2025).
[239] Terry, *supra* n.187.
[240] *Id.*
[241] Evelyn Waugh, *What Is Synthetic Identity Theft*, Experian (Jan. 10, 2024), available at https://www.experian.com/blogs/ask-experian/what-is-synthetic-identity-fraud-theft/.
[242] *The Nightmare of Fake Identities*, Texas Capital, https://texascapitalbank.com/insights/october-2024-synthetic-identity-fraud (last visited July 23, 2025).

241. Importantly, "[f]raudsters can use a multitude of PII elements to create a synthetic identity."[243] Common elements used in synthetic identity theft include SSN, name, date of birth, and other government-issued identifiers, such as a passport or tax identification number.[244]

242. Due to the rise of synthetic identity fraud—which is "a rapidly accelerating threat"[245]—a cybercriminal can capitalize on just one piece of a victim's PII to create a synthetic identity, which they can then use "to apply for and obtain various loans, bank accounts, credit cards and more," or to "file tax returns, obtain medical care or apply for unemployment benefits, all using a fake identity."[246]

243. Unsurprisingly, data breaches are a primary way that "fraudsters gather the information they need to compose a synthetic identity."[247] As CrowdStrike has explained, "[l]arge-scale data breaches expose vast amounts of personal information, which fraudsters then exploit to build synthetic identities."[248]

244. Synthetic identity fraud poses real risks to the real individuals whose information is used to create the synthetic identity. When those real individuals seek credit or otherwise use their identities to facilitate transactions, the synthetic identities often appear as being associated with them. For example, when a minor becomes an adult and seeks to use their SSN to open a bank account, they may be rejected because there is already an account holder with that same SSN. The same issue can arise in the context of credit monitoring, where synthetic identities may become "mixed" with the real account holder's credit information.

---

[243] *How is a synthetic identity created?*, The Fed. Rsrv., https://fedpaymentsimprovement.org/wp-content/uploads/how-is-a-synthetic-identity-created.pdf (last visited July 23, 2025).
[244] *Id.*
[245] Waugh, *supra* n.191.
[246] *What Is Synthetic Identity Theft?*, Equifax, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/synthetic-identity-theft/ (last visited July 23, 2025).
[247] Terry, *supra* n.187.
[248] *Id.*

c. FULLZ PACKAGES

245. In addition, when combined with other publicly available data, any PII element can be used to build full identity profiles, known as "Fullz" packages, which are frequently exploited in financial fraud schemes. "Fullz" is fraudster-speak for data that includes a victim's information, including name, address, SSN, date of birth, and more.

246. With Fullz packages, cybercriminals can cross-reference two (or more) sources of PII to marry unregulated data available elsewhere (e.g., address or phone number) to criminally stolen data to assemble shockingly accurate and complete dossiers on individuals.

247. Compromised PII, whether alone or as part of a Fullz package, is highly valuable to cybercriminals, who can use it to engage in a wide range of fraudulent activities, including committing unemployment insurance fraud, opening unauthorized financial accounts, and applying for government benefits.

248. This type of identity theft renders any compromised data—including seemingly innocuous PII, such as name and contact information—valuable. In the wrong hands, up-to-date names, addresses, phone numbers, and email addresses can be used to update, validate, and verify Fullz packages, which can then be used for nefarious purposes.

249. For example, a fraudster can use an up-to-date Fullz package to bypass identity verification tools—which are often used in financial transactions (like loan applications), background checks, etc.—without detection. In a typical identity verification system, a user submits their PII, like their name, addresses, or date of birth. That customer-submitted PII is then cross-checked against "a trusted data set,"

including those from "credit bureaus, official government documents or mobile operator databases."[249]

250. Thus, with an up-to-date Fullz package—which might include seemingly harmless information, like the identity theft victim's name and current address—a cybercriminal has the victim's up-to-date PII, which will match the victim's information from trusted data sources, like the credit bureaus. With this information, the criminal can then successfully pass identity verification systems without raising any red flags. In this way, Fullz packages, which are made possible by up-to-date and compromised elements of PII, enable fraudsters to carry out various forms of identity theft, including taking out fraudulent loans.

d. SOCIAL SECURITY NUMBER

251. Even when not combined with other data, a SSN is one of the most valuable pieces of personal information, as it can be used to commit a variety of identity theft-related crimes (including, as discussed, synthetic identity theft).

252. For example, criminals can use a stolen SSN to file fraudulent tax returns and claim refunds. This can delay the victim's legitimate tax filing and refund, and result in complications with the IRS. A cybercriminal can also use a stolen SSN to apply for unemployment benefits, Social Security benefits, or other government assistance under the victim's identity, which can affect the victim's legitimate benefits.

253. Criminals can also use SSNs to set up utility services, such as electricity, gas, or internet, in the victim's name, potentially leading to unpaid bills and collections actions. They can likewise use stolen SSNs to rent apartments, lease vehicles, or rent equipment. If the criminal defaults on payments or damages property, the victim may be held financially responsible.

[249] Gus Tomlinson, *What is identity verification and how does it work?*, GBG, https://www.gbg.com/en/blog/what-is-identity-verification-and-how-does-it-work/ (last visited July 23, 2025).

254. Moreover, a cybercriminal can use a stolen SSN to get a job,[250] which can cause problems for the victim with the IRS, wreak havoc on their Social Security benefits, and raise issues in their future employment background checks.[251]

255. In addition, a criminal can use a SSN to open credit card accounts, apply for loans, or create new bank accounts in the victim's name. This can lead to debt and damage to the victim's credit score.

256. SSN theft is particularly distressing because a SSN cannot easily be replaced. In order to obtain a new SSN, a breach victim must demonstrate ongoing harm from misuse of their SSN.[252] In other words, the victim cannot obtain a new SSN until after they have experienced (and documented their) harm. This makes it difficult for individuals whose SSNs have been breached to do anything proactive to avoid identity fraud.

257. Worse yet, even once SSN-related identity theft has occurred and been detected, it is difficult to clean up. For example, in some cases, minors victimized by SSN theft are unfairly treated as complicit in the fraud, especially when fraudulent tax filings, debts, or criminal records are attached to their identities.[253]

---

[250] *Your Social Security Number*, State of Calif. Dept. of Justice, https://oag.ca.gov/idtheft/facts/your-ssn (last visited July 23, 2025).

[251] Gayle Soto, *What Is Employment Identity Theft?*, Experian (Sept. 7, 2024), available at https://www.experian.com/blogs/ask-experian/what-is-employment-identity-theft/.

[252] Blake Stimac, *You Can Change Your Social Security Number, but You Need a Good Reason To. What to Know*, CNET (Oct. 26, 2024), available at https://www.cnet.com/personal-finance/you-can-change-your-social-security-number-but-you-need-a-good-reason-to-what-to-know/ ("If you're an identity theft victim requesting a new Social Security number, you must show that you are experiencing ongoing fraud and also continuing to be negatively impacted by the incidents, such as hits on your credit report. In addition, you must show that you've made attempts to solve the problem through other official means.").

[253] *Protecting Your Kids From Synthetic Identity Fraud*, The Fed. Rsrv., https://fedpaymentsimprovement.org/wp-content/uploads/protect-kids-from-synthetic-identity-fraud.pdf at 1 (last visited July 23, 2025) ("[O]nce fraud is discovered, the burden of proof will likely be on you to convince the credit bureaus and financial institutions that the SSN belongs to your child and not the synthetic identity. This is because the industry typically assumes the first person to establish credit under an SSN is the legitimate owner."); *Synthetic Identity Fraud in the U.S. Payment System*, The Federal Reserve (July 2019), https://fedpaymentsimprovement.org/wp-

Footnote continued on next page

e. NAME AND ADDRESS CAN BE USED TO COMMIT FRAUD

258. While a SSN might be perceived as a uniquely valuable standalone piece of PII to a cybercriminal, the theft of perhaps less sensitive PII, like name and address, can have similarly devastating impacts on victims.

259. Criminals can use a person's name to craft convincing scam letters, emails, or phone calls. For instance, a criminal might send an identity theft victim a bogus tax notification, at the victim's home address, that demands immediate payment.[254] In this way, they can obtain additional details, like the victim's bank account information or SSN.

260. Criminals can also use name and address information to change the victim's address with the U.S. Postal Service and redirect the victim's mail to another location. This allows the bad actors to steal financial statements, credit card offers, and other documents that contain sensitive information, like bank and credit card statements, that arrive via mail.[255]

261. The exposure of seemingly innocuous PII can also lead to additional risks for minors. For instance, with their name and home address stolen in a breach, a child may be at greater risk of stalking, kidnapping, or other physical harm. Demonstrating the sensitive nature of such information when minors are involved, the Children's Online Privacy Protection Act and its implementing rule regulate how young children's PII, including name and home address information, can be collected online.[256]

---

content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf at 17 ("Credit bureaus and financial institutions generally presume that the first individual to establish credit under a given SSN is the valid SSN holder. As a result, the real individual whose SSN has been used in synthetic identity fraud will be faced with the arduous task of proving his or her identity and taking steps to clean up his or her credit report.").

[254] Amy Bunn, *Can Thieves Steal Identities With Only a Name and Address?*, McAfee (March 19, 2024), available at https://www.mcafee.com/blogs/privacy-identity-protection/can-thieves-steal-identities-with-only-a-name-and-address/.

[255] *Id.*

[256] 16 C.F.R. § 312, *et seq*.

f. PROTECTED HEALTH INFORMATION

262. Theft of PII is even more serious when it includes theft of PHI. Where, as here, student data is breached, such PHI included medical records, IEPs for students with special needs, vaccination records, and insurance information.[257] Data breaches involving such medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[258]

263. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[259] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use stolen PII and PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[260] The FTC also warns, "[i]f the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[261]

264. A report published by the World Privacy Forum[262] describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These

---

[257] *Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*, GAO (Sept. 2020), https://www.gao.gov/assets/710/709463.pdf at 12.

[258] Patrick Lucas Austin, "*It Is Absurd." Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), available at https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[259] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), available at https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[260] See FBI, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014) at 14, https://publicintelligence.net/fbi-health-care-cyber-intrusions/.

[261] *See What to Know About Medical Identity Theft*, FTC, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited July 23, 2025).

[262] Dixon & Emerson, *supra*, n.209.

changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services not sought or received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

265. What's more, a 2020 report from the U.S. Government Accountability Office on data breaches in K-12 schools concluded that the disclosure and misuse of a minor's medical records—for example, their diagnoses and special education status—could lead to embarrassment or stigmatization.[263]

2. VICTIMS OF A DATA BREACH ARE HARMED IMMEDIATELY *AND* INDEFINITELY

266. Individuals whose PII is exposed in a data breach are immediately vulnerable to identity theft. The thieves that stole their data in the first instance, like

[263] *Id.*

ShinyHunters here, may themselves use the stolen data to engage in fraudulent transactions.[264] Thus, even if stolen PII does not end up in the hands of criminals other than those who first obtained it, victims of a data breach are nonetheless at risk of identity theft.

a. STOLEN PII IS OFTEN SOLD OR POSTED, AGAIN AND AGAIN

267. The reality, however, is that the data breach victim's information does often end up in the hands of criminals. Cyberthieves routinely sell stolen data on the dark web or to known buyers, and trade the data directly with one another.[265]

268. According to the Department of Health and Human Services, stolen data has a long life cycle, and "tends to filter down through communities, eventually landing in open forums or large marketplaces."[266] "Data is sold and resold, traded and re-traded, repackaged, many times."[267] For example, in one potential life cycle, stolen data is:

- Traded between close associates or sold to known buyers
- Posted for sale in closed forums with high barriers to entry
- Posted for sale in closed forums with lower barriers to entry
- Posted for sale on multi-good marketplaces
- Posted for free on forums
- Posted for free on paste sites[268]

---

[264] Robins-Early, *supra* n.97.

[265] Reza Rafati, *Types of Data Cybercriminals Sell on the Dark Web*, ThreatIntelligenceLab.com (June 22, 2024), available at https://threatintelligencelab.com/blog/types-of-data-cybercriminals-sell-on-the-dark-web/.

[266] *The Dark Web and Cybercrime*, HHS Cybersecurity Program at 10 (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf .

[267] *Id*.

[268] *Id*.; *see also* Nicole Beaudoin, *The danger of data breaches – what you really need to know*, WebRoot (April 22, 2025), available at https://www.webroot.com/blog/2025/04/22/the-danger-of-data-breaches-what-you-really-need-to-know/ ("Data reuse and repurposing: It's important to remember that your stolen information can be used for fraud and theft even years after a data breach…").

269. Stolen data often makes its way to the dark web. The anonymity provided by the dark web has led to a number of markets which traffic in illegal merchandise, including data acquired in a data breach.[269]

270. Once such data is stolen, it is packaged and sold in bulk on dark web marketplaces, which "operate like eBay or Amazon but for illegal goods and services."[270] "Sellers list their 'products'—stolen data—and buyers bid on them."[271]

271. Once stolen data reaches the dark web, it takes on a life of its own. In 2015, researchers at BitGlass created a list of 1,568 phony names, SSNs, credit card numbers, addresses, and phone numbers, placed them in an Excel spreadsheet and then "watermarked" it with their code that silently tracks any access to the file.[272] They then released this fake data on the dark web. From there, the data quickly spread around the world: "[I]t took just 12 days for the data to be clicked more than 1,081 times in 22 different countries, in 5 different continents."[273] Ultimately, the data was downloaded by 47 different parties.[274]

---

[269] *Crime and the Deep Web*, Stevenson University Online, https://www.stevenson.edu/online/about-us/news/crime-deep-web/ (last visited July 23, 2025).

[270] *Dark Web Diaries: What Happens to Your Data After It's Stolen?*, BrandDefense (Oct. 16, 2024), available at https://brandefense.io/blog/dark-web/dark-web-diaries-what-happens-to-your-data/.

[271] *Id.*

[272] Kelly Jackson Higgins, *What Happens When Personal Information Hits the Dark Web*, Dark Reading (April 7, 2015), available at https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web.

[273] Pierluigi Paganini, *How Far do Stolen Data Get in the Deep Web After a Breach?*, Security Affairs (April 12, 2015), available at https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[274] Jackson Higgins, *supra* n.222.

b. HACKERS MAY WAIT YEARS TO STRIKE; IT CAN ALSO TAKE YEARS TO DISCOVER OR RESOLVE IDENTITY FRAUD

272. Even if a data breach victim's stolen PII remains only in the hands of the hackers who first obtained it, the victim still experiences real and lasting harm, as the hackers may wait years, if not decades, to utilize the stolen data.[275]

273. Likewise, even if a cybercriminal begins engaging in identity theft right after obtaining a victim's stolen data, their criminal activity can go undetected for months or even years.[276] For example, minors do not typically engage in activities—like taking out loans or opening accounts—that might flag identity fraud, criminals,[277] enabling criminals to exploit a stolen minor's SSN to create synthetic identities or open fraudulent accounts without immediate detection.[278] This allows fraudulent credit activity to flourish undetected until the child comes of age and attempts to use their

[275] Umang Mehta, *Issue #17: Data Stolen from You May Not be Used Right Away* (Oct. 23, 2024), available at https://www.linkedin.com/pulse/issue-17-data-stolen-from-you-may-used-right-away-umang-mehta-1htgf/; Nicole Martin, *Your Data On The Dark Web Could Dstroy Your Credit Years From Now*, Forbes (updated Oct. 24, 2019), available at https://www.forbes.com/sites/nicolemartin1/2019/10/23/your-data-on-the-dark-web-qa-with-imageware-systems-cto-david-harding.

[276] Hari Ravichandran, *How Long Does It Take To Recover From Identity Theft*, Aura (Aug. 28, 2024), available at https://www.aura.com/learn/how-long-does-it-take-to-recover-from-identity-theft.

[277] *Child Identity Fraud: a Web of Deception and Loss*, Javelin (Nov. 2021), https://javelinstrategy.com/sites/default/files/files/reports/21-5012J-FM-2021%20Child%20Identity%20Fraud%20Study_1.pdf at 10 ("Children aren't filing taxes, taking out loans, paying bills, or opening accounts that require credit checks, the types of activities that often flag identity theft and fraud. So the use of a child's identity to commit crimes is not readily detectable.").

[278] Fed. Rsrv., *supra* n.203 at 17 ("The consequences of synthetic identity fraud on consumers, particularly vulnerable populations (e.g., children, the homeless, the elderly), may not be identified until years after their PII was compromised."); Javelin, *supra* n.227 ("[C]hildren are even easier targets, because they don't understand safe online behaviors, and the compromise of their identities could go on for years before it's detected.").

credit for the first time, often for student loans, employment background checks, or apartment rentals.[279]

274. Finally, even when detected and seemingly resolved, the risks of identity theft are never fully in the past. That is, victims of identity theft may spend significant time and resources untangling the web of fraud, only to find new fraudulent activities surface later on. Indeed, in a 2018 survey, one in four victims of child identity theft reported that they were still dealing with the consequences more than *ten years* after the fact.[280]

P. POWERSCHOOL HAS FAILED TO OFFER ADEQUATE REMEDIES TO PROTECT STUDENTS AND EDUCATORS

275. Following the Data Breach, PowerSchool offered educators and adult students whose information was compromised a short window to enroll in two years of complimentary identity protection and credit monitoring services ("Option 1").[281] Meanwhile, for young students whose information was compromised, PowerSchool offered complimentary identity protection services only ("Option 2").[282]

276. Both Options, however, are insufficient. Fundamentally, credit monitoring and identity protection services merely alert consumers of fraudulent activity. In order for such services to provide any value, consumers must then spend time reviewing the alerts (which can be confusing), and navigating and executing next steps (which can be time-consuming). For example, credit monitoring does not correct

---

[279] *Identity Theft: Child Identity Theft*, Georgia Attorney General's Consumer Protection Division, https://consumer.georgia.gov/consumer-topics/identity-theft-child-identity-theft (last visited July 23, 2025) ("Unfortunately, children and adolescents have become one of the fastest growing sectors of identity theft victims. And often the crime is not discovered until years after the initial theft occurs, when a young adult is applying to college, for a job or for a credit card for the first time.").

[280] *Experian launches free service to detect child identity theft*, PR Newswire (Aug. 27, 2018), available at https://www.prnewswire.com/news-releases/experian-launches-free-service-to-detect-child-identity-theft-300702344.html.

[281] Breach Notice; https://www.experianidworks.com/plus.

[282] Breach Notice; https://www.experianidworks.com/minorplus.

credit report errors, file fraud reports, or initiate credit freezes—only a consumer can do that.[283] These services therefore place the burden of risk mitigation on consumers. Thus, while credit monitoring and identity protection services may be helpful tools, they are "not a holistic approach to preventing identity theft or unauthorized transactions."[284]

277. Moreover, in offering Option 1 and Option 2—both of which require a user to provide their PII to enroll—PowerSchool ignores the fact that many impacted educators and families have lost all trust in PowerSchool. Indeed, one study found that 65% of data breach victims lost trust in an organization after a data breach, while another found that 80% of consumers in developed nations will defect from a business if their information is compromised in a breach.[285] Such studies suggest that many teachers and families will be hesitant to enroll in a PowerSchool-sponsored credit monitoring and/or identity protection serves, rendering Options 1 and 2—which, even if used, are of limited utility.

278. Aside from these central flaws, Options 1 and 2 do not protect impacted students and teachers from the harms they now inevitably, and indefinitely, face as a result of the Data Breach. Both offerings suffer from critical omissions and design flaws that undermine the utility of the credit monitoring and/or identity protection services.

279. **Short Duration (Despite Long-Term Risks).** Both Options 1 and 2 are limited to two years. This limited window is misaligned with the nature of SSN-related fraud, which can unfold over decades. A breach victim's stolen identity might be

---

[283] Amanda Garland, *What is credit monitoring?*, Bankrate (Oct. 31, 2024), available at https://www.bankrate.com/personal-finance/credit/credit-monitoring-when-is-it-worth-paying-for/#how-it-works.

[284] Alexandria White, *What is credit monitoring and how does it protect you from fraud?*, CNBC (updated Aug. 5, 2025), available at https://www.cnbc.com/select/what-is-credit-monitoring/.

[285] Tilly Kenyon, *What causes the most damage, losing data or trust?*, Cyber Magazine (June 22, 2021), available at https://cybermagazine.com/cyber-security/what-causes-most-damage-losing-data-or-trust.

dormant in criminal networks many years before it is exploited, meaning that the protection PowerSchool offers could expire long before the threat does. Many forms of fraud such as tax refund theft, synthetic identity creation, and benefits fraud may not occur immediately but surface long after credit monitoring and/or identity protection ends. Indeed, for minor victims of a data breach, fraudsters routinely wait a decade or more, until the victim is old enough to apply for student loans, credit cards, or rental agreements, before activating stolen identities, knowing that the victim likely has no idea their SSN was ever compromised. Despite these long-term risks, PowerSchool makes no provision for post-expiration alerts, renewals, or financial assistance to continue identity protection and/or credit monitoring once the two-year window closes. Impacted educators and students may therefore be lulled into complacency, believing their risk ends when the service expires, when in fact the risk has only just begun.

280. **The Services are Reactive, Not Proactive.** Both offerings are primarily reactive, focusing on detecting and responding to identity theft, rather than preventing it from occurring in the first place. For example, neither Option 1 or 2 includes automatic credit freezes, which essentially locks a credit file until the freeze is lifted, making it significantly more difficult for identity thieves to use stolen SSNs to open new accounts. All told, a credit freeze is one of the most effective ways to block fraudulent credit activity before it starts. However, aside from providing basic information about credit freezes to those impacted by the Breach,[286] PowerSchool has done nothing further to provide direct assistance to facilitate the process of signing up for credit freezes with major credit bureaus. Additionally, Option 1 and 2 do not incorporate credit monitoring tools that detect early warning signs of identity misuse, such as frequent credit inquiries or data matches in public records. Providing proactive protection would better align with the level of risk posed by long-term exposure of sensitive information.

[286] Breach Notice.

Q. PLAINTIFFS' EXPERIENCES OR INJURIES

1. EMPLOYEES

a. GEORGIA TEACHER CHARLOTTE RENN

281. Plaintiff Charlotte Renn ("Plaintiff Renn") is a citizen and resident of Georgia. At all relevant times, Plaintiff Renn was employed by Floyd County School District, which used PowerSchool's SIS. Plaintiff Renn has been employed by Floyd County School District going on her ninth year. As a condition of Plaintiff Renn's employment, Plaintiff Renn's school district entered highly sensitive PII into PowerSchool's SIS.

282. Plaintiff Renn received an email dated February 26, 2025, notifying Plaintiff Renn of the Data Breach.

283. As a result of the Data Breach and as recommended in the Notice, Plaintiff Renn made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, cancelling and requesting reissuance of multiple credit cards that had fraudulent charges entered, accessing and reviewing credit agency records, freezing and unfreezing credit accounts, and maintaining diligent review of her banking and other accounts.

284. Plaintiff Renn has spent significant time responding to the Data Breach, including several hours of phone calls and research, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, child care and/or recreation. Plaintiff Renn suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

285. PowerSchool was legally obligated to protect Plaintiff Renn's PII. Plaintiff Renn would not have allowed her PII to be shared with or accessible by

PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

286. Thus, as a result of the Data Breach, Plaintiff Renn has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Renn has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

b. INDIANA TEACHER KIMBERLY KINNEY

287. Plaintiff Kimberly Kinney ("Plaintiff Kinney") is a citizen and resident of Indiana. At all relevant times, Plaintiff Kinney was employed by Brownsburg Community School Corporation, which used PowerSchool's SIS. Plaintiff Kinney has been employed by Brownsburg Community School Corporation since July 2017. As a condition of Plaintiff Kinney's employment, Plaintiff Kinney was required to enter highly sensitive PII into PowerSchool's SIS.

288. Plaintiff Kinney received an email dated January 8, 2025, notifying her of the Data Breach.

289. As a result of the Data Breach and as recommended in the Notice, Plaintiff Kinney made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

290. Plaintiff Kinney has spent significant time responding to the Data Breach, including addressing a marked increase in spam communications and several hours of phone calls, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Kinney suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy, the potential appearance of her data on the dark web, and potential

further damages over the impact of cybercriminals accessing and using their PII and PHI. She is concerned about the impact of the Data Breach on her students, their families, and her fellow teachers whose data was also exposed.

291. PowerSchool was legally obligated to protect Plaintiff Kinney's PII. Plaintiff Kinney would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

292. Thus, as a result of the Data Breach, Plaintiff Kinney has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Kinney has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

c. NORTH CAROLINA EMPLOYEE KIMBERLY GREER

293. Plaintiff Kimberly Greer ("Plaintiff Greer") is a citizen and resident of North Carolina. At all relevant times, Plaintiff Greer was employed by Winston-Salem/Forsyth County Schools, which used PowerSchool's SIS. Plaintiff Greer has been employed by Winston-Salem/Forsyth County Schools since August 2022 as a Social Worker. As a condition of Plaintiff Greer's employment, Plaintiff Greer was required to enter highly sensitive PII into PowerSchool's SIS, including but not limited to her date of birth, social security number, home address, email, and phone number.

294. Plaintiff Greer received an email on February 4, 2025, notifying Plaintiff Greer about the Data Breach.

295. As a result of the Data Breach and as recommended in the Notice, Plaintiff Greer made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing her financial and credit

accounts for fraudulent activity. On June 11, 2025, Experian Identity Works notified Plaintiff Greer that her email address was found on the dark web.

296. Plaintiff Greer has spent significant time, including several hours of phone calls responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation. Plaintiff Greer suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

297. PowerSchool was legally obligated to protect Plaintiff Greer's PII. Plaintiff Greer would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

298. Thus, as a result of the Data Breach, Plaintiff Greer has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Greer has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

d. NORTH CAROLINA TEACHER JUSTINE SHAMEY

299. Plaintiff Justine Shamey ("Plaintiff Shamey") is a citizen and resident of North Carolina. At all relevant times, Plaintiff Shamey was employed by Winston-Salem Forsyth County School District, which used PowerSchool's SIS. Plaintiff Shamey has been employed as a teacher by Winston-Salem Forsyth County School District since August 2021. As a condition of Plaintiff Shamey's employment, Plaintiff Shamey was required to enter highly sensitive PII into PowerSchool's SIS.

300. Plaintiff Shamey received an email dated January 8, 2025, notifying her of the Data Breach.

301. As a result of the Data Breach and as recommended in the Notice, Plaintiff Shamey made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, maintaining diligent review of her banking and other accounts for unusual or unauthorized charges.

302. Plaintiff Shamey has spent significant time responding to the Data Breach, including time spent reviewing and securing financial accounts, managing an increase of spam phone calls, texts messages, and emails, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare and/or recreation. Plaintiff Shamey suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

303. PowerSchool was legally obligated to protect Plaintiff Shamey's PII. Plaintiff Shamey would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

Thus, as a result of the Data Breach, Plaintiff Shamey has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Shamey has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

e. NORTH CAROLINA TEACHER CHRISTOPHER JOSEPH WAGONER

304. Plaintiff Christopher Joseph Wagoner ("Plaintiff Wagoner") is a citizen and resident of North Carolina. At all relevant times, Plaintiff Wagoner was employed by the Bladen County School District, which used PowerSchool's SIS. Plaintiff Wagoner has been employed by Bladen County School District since October 2022.

As a condition of Plaintiff Wagoner's employment as a math and science teacher, Plaintiff Wagoner was required to enter highly sensitive PII into PowerSchool's SIS.

305. Plaintiff Wagoner received an email dated February 28, 2025, notifying Plaintiff Wagoner of the Data Breach.

306. As a result of the Data Breach and as recommended in the Notice, Plaintiff Wagoner made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

307. Plaintiff Wagoner has spent significant time responding to the Data Breach, including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, and/or recreation. Plaintiff Wagoner suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII.

308. PowerSchool was legally obligated to protect Plaintiff Wagoner's PII. Plaintiff Wagoner would not have allowed his PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect his PII.

309. Thus, as a result of the Data Breach, Plaintiff Wagoner has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Wagoner has a continuing interest in ensuring that his PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

f. OKLAHOMA TEACHER PAUL GARRETH THOMPSON

310. Plaintiff Paul Garreth Thompson ("Plaintiff Thompson") is a citizen and resident of Oklahoma. At all relevant times, Plaintiff Thompson was employed by Epic Charter Schools, which used PowerSchool's SIS. Plaintiff Thompson was employed by Epic Charter Schools since 2020. As a condition of Plaintiff Thompson's employment as a teacher at Epic Charter Schools, highly sensitive PII regarding Plaintiff Thompson was input into PowerSchool's SIS.

311. Plaintiff Thompson received an email dated March 1, 2025, notifying him about the Data Breach.

312. As a result of the Data Breach and as recommended in the Notice, Plaintiff Thompson made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

313. Plaintiff Thompson has spent significant time responding to the Data Breach, including addressing a noticeable increase in spam calls, text and email messages that interfere with work duties and personal time, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, and/or recreation. Plaintiff Thompson suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII.

314. PowerSchool was legally obligated to protect Plaintiff Thompson's PII. Plaintiff Thompson would not have allowed his PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect his PII.

Thus, as a result of the Data Breach, Plaintiff Thompson has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Thompson has a continuing interest in ensuring that his PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

g. RHODE ISLAND TEACHER DENISE CHAMPNEY

315. Plaintiff Denise Champney ("Plaintiff Champney) is a citizen and resident of Rhode Island. At all relevant times, Plaintiff Champney was employed by the Chariho School District, which used PowerSchool's SIS. Plaintiff Champney was employed by Chariho School District since August of 2017. As a condition of Plaintiff Champney's employment as a Speech Language Pathologist at the Chariho School District, Plaintiff Champney was required to enter highly sensitive PII into PowerSchool's SIS.

316. Plaintiff Champney received an email dated January 8, 2025, notifying Plaintiff Champney of the Data Breach.

317. As a result of the Data Breach and as recommended in the Notice, Plaintiff Champney made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

318. Plaintiff Champney has spent significant time, including several hours of phone calls, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, and/or recreation. Plaintiff Champney suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

319. PowerSchool was legally obligated to protect Plaintiff Champney's PII. Plaintiff Champney would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

320. Thus, as a result of the Data Breach, Plaintiff Champney has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Champney has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

h. VERMONT EMPLOYEE MICHELE BALLARD

321. Plaintiff Michele Ballard ("Plaintiff Ballard") is a citizen and resident of Vermont. At all relevant times, Plaintiff Ballard was employed by Montpelier Roxbury Public Schools, which used PowerSchool's SIS. Plaintiff Ballard has been employed by Montpelier Roxbury Public Schools since 2023**.** Plaintiff Ballard was previously employed at Harwood Unified Union School District from 1998 to 2023, which also used PowerSchool's SIS. As a condition of Plaintiff Ballard's employment, Plaintiff Ballard was required to enter sensitive PII into PowerSchool's SIS, including but not limited to her role, email address, phone number, address, and dates of employment.

322. Plaintiff Ballard received an email dated February 25, 2025, notifying Plaintiff Ballard of the Data Breach.

323. As a result of the Data Breach and as recommended in the Notice, Plaintiff Ballard made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

324. Plaintiff Ballard has spent time responding to the Data Breach, including addressing a noticeable increase in spam text messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have

spent on other activities, including, but not limited to, work, and/or recreation. Plaintiff Ballard suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

325. PowerSchool was legally obligated to protect Plaintiff Ballard's PII. Plaintiff Ballard would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

Thus, as a result of the Data Breach, Plaintiff Ballard has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Ballard has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

i. VIRGINIA TEACHER DUSTY LYNN JENKINS SPENCE

326. Plaintiff Dusty Lynn Jenkins Spence ("Plaintiff Spence") is a citizen and resident of Virginia. At all relevant times, Plaintiff Spence was employed by Blacksburg High School, which used PowerSchool's SIS. Plaintiff Spence has been employed by Blacksburg High School since August 2021. As a condition of Plaintiff Spence's employment, Plaintiff Spence is informed and believes that Blacksburg High School was required to enter her sensitive PII into PowerSchool's SIS.

327. Plaintiff Spence received an email dated March 2, 2025, notifying Plaintiff Spence of the Data Breach.

328. As a result of the Data Breach and as recommended in the Notice, Plaintiff Spence made reasonable efforts to mitigate the impact of the Data Breach, including,

but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

329. Plaintiff Spence has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. She has spent hours dealing with increased spam calls, text messages, and emails. Shortly after the Data Breach occurred, Plaintiff Spence's bank notified her that her checking account had been hacked. She had to close her account and open a new one, spending hours updating her automated billing and account information. Plaintiff Spence suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII and PHI.

330. PowerSchool was legally obligated to protect Plaintiff Spence's PII. Plaintiff Spence would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

Thus, as a result of the Data Breach, Plaintiff Spence has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Spence has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

2. EMPLOYEE AND MINOR STUDENT

a. ARIZONA TEACHER WILLIAM JEREMIAH TARBUSH AND MINOR STUDENT A.C.T.

331. Plaintiffs William Jeremiah Tarbush ("Plaintiff Tarbush") and his minor child A.C.T. ("Plaintiff A.C.T.") are citizens and residents of Arizona. At all relevant

times, Plaintiff A.C.T. was a student at Leman Academy of Excellence, which used PowerSchool's SIS. At all relevant times, Plaintiff Tarbush was a teacher employed by CPLC Community Schools. Plaintiff A.C.T. was enrolled at Leman Academy of Excellence from 2017 to 2021. Plaintiff Tarbush was employed by CPLC Community Schools from July 24, 2023, to April 11, 2026. As a condition of Plaintiff A.C.T.'s enrollment as a student at Leman Academy of Excellence, and as a condition of Plaintiff Tarbush's employment with CPLC Community Schools, Plaintiffs Tarbush and A.C.T.'s PII were input into PowerSchool's SIS.

332. Plaintiff Tarbush received an alert dated January 15, 2025, notifying him about the Data Breach.

333. As a result of the Data Breach and as recommended in the Notice, Plaintiff Tarbush made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor child's PII.

334. Plaintiff Tarbush has spent significant time responding to the Data Breach on behalf of himself and Plaintiff A.C.T., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Tarbush suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiff A.C.T.'s PII.

335. PowerSchool was legally obligated to protect Plaintiffs Tarbush and A.C.T.'s PII. Plaintiff Tarbush would not have allowed his family's PII to be shared with or accessible by PowerSchool if Plaintiff Tarbush had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

Thus, as a result of the Data Breach, Plaintiffs Tarbush and A.C.T. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Tarbush and A.C.T. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

b. MASSACHUSETTS EMPLOYEE JONATHAN NEWELL AND MINOR STUDENTS B.R.N. AND B.D.N.

336. Plaintiff Jonathan Newell ("Plaintiff Newell") and his minor children B.R.N. ("Plaintiff B.R.N." and B.D.N. ("Plaintiff B.D.N.") are citizens and residents of Woburn, Massachusetts. At all relevant times, Plaintiff Newell was a school counselor at Prospect Hill Academy Charter School, which used PowerSchool's SIS. Plaintiff Newell was employed as a school counselor at Prospect Hill Academy Charter school from September 2023 until the present. As a condition of Plaintiff Newell's employment, Plaintiff Newell's PII was input into PowerSchool's SIS.

337. Plaintiffs B.R.N. and B.D.N. are students at Woburn High School and Hurld Wyman Elementary School in Woburn, Massachusetts, which used PowerSchool's SIS at all relevant times. Plaintiff B.R.N. was enrolled in Woburn High School from September 2024 until the present and Plaintiff B.D.N. was enrolled in Hurld Wyman Elementary School from September 2020 until June 2026. As a condition of Plaintiffs B.R.N. and B.D.N.'s enrollment, Plaintiff Newell's PII and his children's PII and PHI were input into PowerSchool's SIS.

338. Plaintiff Newell received an email dated January 9, 2025, notifying him of the Data Breach. Plaintiff Newell also received an email from the Woburn School District notifying him of the Data Breach.

339. As a result of the Data Breach and as recommended in the Notice, Plaintiff Newell made reasonable efforts to mitigate the impact of the Data Breach, including,

but not limited to, researching the Data Breach, maintaining diligent review of his family's banking and other accounts, and seeking to protect his own and his minor children's PII and PHI.

340. Plaintiff Newell has spent significant time responding to the Data Breach on behalf of himself and Plaintiffs B.R.N. and B.D.N., including addressing a noticeable increase in spam calls and messages, and unauthorized charges on his accounts, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Newell suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his and Plaintiffs B.R.N. and B.D.N.'s PII and PHI.

341. PowerSchool was legally obligated to protect Plaintiffs Newell, B.R.N., and B.D.N.'s PII and PHI. Plaintiff Newell would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

Thus, as a result of the Data Breach, Plaintiffs Newell, B.R.N., and B.D.N. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Newell, B.R.N., and B.D.N. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

c. NEW HAMPSHIRE EMPLOYEE KELSEY GAURON AND MINOR STUDENT R.M.M.

342. Plaintiff Kelsey Gauron ("Plaintiff Gauron") and her minor child, R.M.M., are citizens and residents of New Hampshire. At all relevant times, Plaintiff Gauron was employed by Lincoln Akerman School, and R.M.M. was a student at Seabrook Middle School, both in School Administrative Unit 21, which used

PowerSchool's SIS. Plaintiff Gauron has been employed by Lincoln Akerman School as an educational associate for eight years.

343. R.M.M. has been enrolled at Seabrook Middle School since August 2021 and at School Administrative Unit 21 since August 2016. As a condition of Plaintiff R.M.M.'s enrollment as a student at Seabrook Middle School, Plaintiffs Gauron's and R.M.M.'s PII and PHI were input into PowerSchool's SIS, including but not limited to health records, personal information, testing information, addresses, birth certificates, and Social Security Numbers.

344. Plaintiff Gauron received an email dated February 7, 2025, notifying Plaintiff Gauron of the Data Breach.

345. As a result of the Data Breach and as recommended in the Notice, Plaintiff Gauron made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, maintaining diligent review of her banking and other accounts, and seeking to protect her own and her minor child's PII and PHI.

346. Plaintiff Gauron has spent significant time on behalf of herself and Plaintiff R.M., including at least 4 hours of phone calls and research responding to the Data Breach, disputing a credit card she never applied for, disputing charges she did not make, cancelling and requesting reissuance of multiple debit cards that had fraudulent charges entered, dealing with her child support card that was compromised, and accessing and reviewing credit agency records, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, child care and/or recreation. Plaintiff Gauron suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff R.M.M.'s PII and PHI.

347. PowerSchool was legally obligated to protect Plaintiffs Gauron and R.M.M.'s PII and PHI. Plaintiff Gauron would not have allowed her family's PII and PHI to be shared with PowerSchool if she had known PowerSchool would not adequately protect their PII and PHI, including by failing to implement and maintain sufficient data security safeguards to adequately protect their PII and PHI.

Thus, as a result of the Data Breach, Plaintiff Gauron and R.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiff Gauron and R.M. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

d. NEW MEXICO TEACHER KAITLYN GILLIS AND MINOR STUDENT W.C.G.

348. Plaintiff Kaitlyn Michele Gillis ("Plaintiff Gillis") and her minor child W.C.G. ("Plaintiff W.C.G.") are citizens and residents of New Mexico. At all relevant times, Plaintiff Gillis was a teacher at Hatch Valley High School, where she has been teaching since August 2018. As a condition of Plaintiff Gillis' employment, her PII was input into PowerSchool's SIS.

349. At all relevant times, Plaintiff W.C.G. was a student at Garfield Elementary, which used PowerSchool's SIS. Plaintiff W.C.G. has been enrolled at Garfield Elementary since August 2024. As a condition of Plaintiff W.C.G.'s enrollment, Plaintiffs Gillis and W.C.G's PII were input into PowerSchool's SIS, including but not limited to Plaintiff W.C.G.'s full name, Social Security Number, date of birth, and parent contact information.

350. Plaintiff Gillis received an email dated January 20, 2025, from her employer, Hatch Valley Public Schools, notifying her about the Data Breach. On February 28, 2025, Plaintiff Gillis received two emails from PowerSchool – one referencing her name and the other, W.C.G.'s name, describing the Data Breach. On

March 7, 2025, Plaintiff Gillis received an email from Hatch Valley Public Schools' Technology Director, forwarding an email from PowerSchool that included the final CrowdStrike Incident Report.

351. As a result of the Data Breach and as recommended in the Notice, Plaintiff Gillis made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

352. Plaintiff Gillis has spent significant time responding to the Data Breach on behalf of herself and Plaintiff W.C.G., including enrolling herself and Plaintiff W.C.G. in Experian IdentityWorks, checking her credit report and financial account statements, and addressing the fraudulent use of W.C.G.'s identity by an unknown individual who improperly claimed W.C.G. as a dependent on a 2024 federal tax return, all of which interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Gillis suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her and her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff W.C.G.'s PII.

353. PowerSchool was legally obligated to protect Plaintiffs Gillis and W.C.G.'s PII. Plaintiff Gillis would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

Thus, as a result of the Data Breach, Plaintiffs Gillis and W.C.G. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Gillis and W.C.G. have a continuing interest in ensuring that their

PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

3. PARENTS AND MINOR STUDENT

a. ALABAMA PARENT CHRISTINA ASHLEY HARDWICK AND MINOR STUDENT L.D.

354. Plaintiffs Christina Ashley Hardwick ("Plaintiff Hardwick") and her minor child L.D. ("Plaintiff L.D.") are citizens and residents of Alabama. At all relevant times, Plaintiff L.D. was a student in Blount County Schools, which used PowerSchool's SIS. Plaintiff L.D. has been enrolled in Blount County Schools since August 2020. As a condition of Plaintiff L.D.'s enrollment, Plaintiffs Hardwick and L.D.'s PII were input into PowerSchool's SIS, including but not limited to home addresses and Social Security Numbers.

355. Plaintiff Hardwick received an email dated March 21, 2025, notifying Hardwick about the Data Breach.

356. As a result of the Data Breach and as recommended in the Notice, Plaintiff Hardwick made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

357. Plaintiff Hardwick has spent significant time responding to the Data Breach on behalf of herself and Plaintiff L.D., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff L.D.'s personal information was found on the dark web and Plaintiff Hardwick has been working to address the found information. Plaintiff Hardwick suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and

potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff L.D.'s PII.

358. PowerSchool was legally obligated to protect Plaintiffs Hardwick and L.D.'s PII. Plaintiff Hardwick would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

359. Thus, as a result of the Data Breach, Plaintiffs Hardwick and L.D. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Hardwick and L.D. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

b. ALABAMA PARENT VALARIE RENEE RHODEN AND MINOR STUDENT C.A.R.

360. Plaintiffs Valarie Renee Rhoden ("Plaintiff Rhoden") and her minor child C.A.R. ("Plaintiff C.A.R.") are citizens and residents of Alabama. At all relevant times, Plaintiff C.A.R. was a student in Talladega City Schools, which used PowerSchool's SIS. Plaintiff C.A.R. has been enrolled in Talladega City Schools since August 2014. As a condition of Plaintiff C.A.R.'s enrollment, Plaintiffs Rhoden and C.A.R.'s PII and PHI were input into PowerSchool's SIS, including but not limited to addresses, Social Security Numbers, financial information and immunization records.

361. Plaintiff Rhoden received an email dated March 20, 2025, notifying her of the Data Breach.

362. As a result of the Data Breach and as recommended in the Notice, Plaintiff Rhoden made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII and PHI.

363. Plaintiff Rhoden has spent significant time responding to the Data Breach on behalf of herself and Plaintiff C.A.R., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Rhoden suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has experienced issues with receipt of benefits since the Data Breach. Plaintiff Rhoden has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff C.A.R.'s PII and PHI.

364. PowerSchool was legally obligated to protect Plaintiffs Rhoden and C.A.R.'s PII and PHI. Plaintiff Rhoden would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if Plaintiff Rhoden had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

365. Thus, as a result of the Data Breach, Plaintiffs Rhoden and C.A.R. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Rhoden and C.A.R. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

c. CALIFORNIA PARENT DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A.

366. Plaintiff Dobie James August ("Plaintiff August") and his minor children K.J.A. ("Plaintiff K.J.A.") and K.D.A. ("Plaintiff K.D.A.") are citizens and residents of California. At all relevant times, Plaintiffs K.J.A. and K.D.A. were students at Thurgood Marshall Middle School, which used PowerSchool's SIS. Plaintiff K.J.A. was enrolled at Thurgood Marshall Middle School from October 2023 through May

2025. Plaintiff K.D.A has been enrolled at Thurgood Marshall Middle School from October 2023 to present. As a condition of Plaintiffs K.J.A. and K.D.A.'s enrollment, Plaintiffs August, K.J.A., and K.D.A.'s PII were input into PowerSchool's SIS.

367. Plaintiff August received an email dated January 10, 2025, notifying families of the San Diego Unified School District, which includes Thurgood Marshall Middle School, of the Data Breach.

368. As a result of the Data Breach and as recommended in the Notice, Plaintiff August made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor child's PII.

369. Plaintiff August has spent significant time responding to the Data Breach on behalf of himself and Plaintiffs K.J.A. and K.D.A., including researching the Data Breach, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff August suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiffs K.J.A. and K.D.A.'s PII.

370. PowerSchool was legally obligated to protect Plaintiffs August, K.J.A., and K.D.A.'s PII. Plaintiff August would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

371. Thus, as a result of the Data Breach, Plaintiffs August, K.J.A., and K.D.A. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs August, K.J.A., and K.D.A. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

d. CALIFORNIA PARENT DAVID BROWNLEE AND MINOR STUDENT A.B.

372. Plaintiff David Brownlee ("Plaintiff Brownlee") and his minor child A.B. ("Plaintiff A.B.") are citizens and residents of California. At all relevant times, Plaintiff A.B. was a student at Kate Sessions Elementary School or Pacific Beach Middle School, both of which used PowerSchool's SIS. Plaintiff A.B. was enrolled in the San Diego Unified School District since at least August 2018. As a condition of Plaintiff A.B.'s enrollment as a student, Plaintiff Brownlee's PII and Plaintiff A.B.'s PII and PHI were input into PowerSchool's SIS.

373. Plaintiff Brownlee received emails dated January 8 and 10, 2025, notifying Plaintiff Brownlee of the Data Breach.

374. As a result of the Data Breach and as recommended in the Notice, Plaintiff Brownlee made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own PII and his minor child's PII and PHI.

375. Plaintiff Brownlee has spent significant time responding to the Data Breach on behalf of himself and Plaintiff A.B., including several hours of emails and phone calls, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Brownlee has experienced fraud on a credit card which required closing the account, as well as an increase in phishing communications. Plaintiff Brownlee suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using Plaintiff Brownlee's PII and Plaintiff A.B.'s PII and PHI.

376. PowerSchool was legally obligated to protect Plaintiffs Brownlee and A.B's PII and PHI. Plaintiff Brownlee would not have allowed his family's PII to be

shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

377. Thus, as a result of the Data Breach, Plaintiffs Brownlee and A.B. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for Plaintiffs Brownlee and A.B.'s lifetime. Plaintiffs Brownlee and A.B. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

e. CALIFORNIA PARENT NICOLE FLICK AND MINOR STUDENT M.C.

378. Plaintiff Nicole Flick ("Plaintiff Flick") and her minor child M.C. ("Plaintiff M.C.") are citizens and residents of California. At all relevant times, Plaintiff M.C. was a student at Mason Elementary School within the San Diego Unified School District, which used PowerSchool's SIS. Plaintiff M.C. has been enrolled in Mason Elementary School within the San Diego Unified School District since August 2024. As a condition of Plaintiff M.C.'s enrollment as a student, Plaintiff Flick's PII and Plaintiff M.C.'s PII and PHI were input into PowerSchool's SIS to promote interoperability of educational services, specifically M.C.'s date of birth, social security number, medical information, information concerning M.C.'s individualized education plan, and the family's address and phone number which was under Plaintiff Flick's name.

379. Plaintiff Flick received an email dated January 12, 2025, notifying her of the Data Breach.

380. As a result of the Data Breach and as recommended in the Notice, Plaintiff Flick made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her and her minor child's PII and PHI.

381. Plaintiff Flick has spent significant time responding to the Data Breach on behalf of herself and Plaintiff M.C., including dealing with an influx of spam and phishing calls, texts, and emails, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Flick suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff M.C.'s PII and PHI.

382. PowerSchool was legally obligated to protect Plaintiffs Flick and M.C.'s PII. Plaintiff Flick would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

383. Thus, as a result of the Data Breach, Plaintiffs Flick and M.C. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for Plaintiffs Flick and M.C.'s lifetimes. Plaintiffs Flick and M.C. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

f. CALIFORNIA PARENT ASHLEY WRIGHT AND MINOR STUDENT A.N.B.

384. Plaintiff Ashley Wright ("Plaintiff Wright") and her minor child A.N.B. ("Plaintiff A.N.B.") are citizens and residents of California. At all relevant times, Plaintiff A.N.B. was a student at West Contra Costa Unified School District, which used PowerSchool's SIS. Plaintiff A.N.B. has been enrolled in the West Contra Costa Unified School District ("WCCUSD") since August 2019. As a condition of Plaintiff A.N.B.'s enrollment, Plaintiffs Wright and A.N.B.'s PII were input into PowerSchool's SIS.

385. Plaintiff Wright received an email dated January 10, 2025, notifying "the WCCUSD Community" about the Data Breach.

386. As a result of the Data Breach and as recommended in the Notice, Plaintiff Wright made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

387. Plaintiff Wright has spent significant time responding to the Data Breach on behalf of herself and Plaintiff A.N.B., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Wright has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff A.N.B.'s PII.

388. PowerSchool was contractually and legally obligated to protect Plaintiffs Wright and A.N.B.'s PII once it was provided to PowerSchool. Plaintiff Wright would not have provided her family's PII to PowerSchool if Plaintiff Wright had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

389. Thus, as a result of the Data Breach, Plaintiffs Wright and A.N.B. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Wright and A.N.B. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

g. CALIFORNIA PARENT DAVID ZARATE AND MINOR STUDENT A.Z.

390. Plaintiff David Zarate ("Plaintiff Zarate") and his minor child A.Z. ("Plaintiff A.Z.") are citizens and residents of California. At all relevant times, Plaintiff A.Z. was a student at the West Contra Costa Unified School District, which used PowerSchool's SIS. Plaintiff A.Z. first enrolled in the West Contra Costa Unified School District in July 2024. As a condition of Plaintiff A.Z.'s enrollment, Plaintiff Zarate's PII and Plaintiff A.Z.'s PII and PHI were input into PowerSchool's SIS, specifically A.Z.'s date of birth, social security number, and medical and dental information, and the family's home address and phone number.

391. Plaintiff Zarate received an email dated February 24, 2025, notifying him of the Data Breach.

392. As a result of the Data Breach and as recommended in the Notice, Plaintiff Zarate made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his PII and his minor child's PII and PII. He purchased identity theft protection from Norton/Lifelock at a personal cost of $155 per year. He also placed a freeze on Plaintiff A.Z.'s credit, which may prevent some—but not all—types of fraud of which Plaintiff A.Z. is now at risk.

393. Plaintiff Zarate has spent significant time responding to the Data Breach on behalf of himself and Plaintiff A.Z., including approximately 40 hours contacting various institutions including PowerSchool, the California Privacy Protection Agency, the Federal Trade Commission, California Attorney General, United States Department of Education, and Experian; and researching various credit and identity theft monitoring services, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Zarate suffered lost time, annoyance, interference, emotional

distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own PII and Plaintiff A.Z.'s PII and PHI.

394. PowerSchool was legally obligated to protect Plaintiffs Zarate and A.Z.'s PII. Plaintiff Zarate would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

395. Thus, as a result of the Data Breach, Plaintiffs Zarate and A.Z. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Zarate and A.Z. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

h. FLORIDA PARENT DAVID SAUVE AND MINOR STUDENT A.S.

396. Plaintiff David Sauve ("Plaintiff Sauve") and his minor child A.S. ("Plaintiff A.S.") are citizens and residents of Florida. At all relevant times, Plaintiff A.S. was a student at PM Wells Charter Academy, which used PowerSchool's SIS. Plaintiff A.S. was enrolled in the PM Wells Charter Academy for the 2019 and 2020 school years. As a condition of Plaintiff A.S.'s enrollment as a student at PM Wells Charter Academy, Plaintiff Sauve's PII and Plaintiff A.S.'s PII and PHI were input into PowerSchool's SIS, specifically A.S.'s date of birth, physician contact, and immunization records, and the family's address and phone number under Plaintiff Sauve's name.

397. Plaintiff Sauve received an email dated March 2, 2025, notifying him of the Data Breach.

398. As a result of the Data Breach and as recommended in the Notice, Plaintiff Sauve made reasonable efforts to mitigate the impact of the Data Breach, including,

but not limited to, researching the Data Breach and seeking to protect his own and his minor child's PII and PHI.

399. Plaintiff Sauve has spent significant time responding to the Data Breach on behalf of himself and Plaintiff A.S. and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, and/or recreation. Shortly after and as a result of the breach, Plaintiff Sauve experienced an extreme increase in spam phone calls, spam text messages, and phishing emails. He has had two banking accounts compromised, requiring him to spend several hours on the phone with banks closing accounts. He experienced fraud on one of his accounts, specifically Plaintiff Sauve's bank verified Plaintiff Sauve's fraud claim which took place on May 24, 2025, in the amount of $78.99. Plaintiff Sauve has received multiple fraud alerts from CreditKarma, Rocketmoney, and Experian, including notification that his PII is available on the dark web. Plaintiff Sauve has suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own PII and Plaintiff A.S.'s PII and PHI.

400. PowerSchool was legally obligated to protect Plaintiffs Suave and A.S.'s PII and PHI. Plaintiff Suave would not have allowed his family's PII and PHI to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

401. Thus, as a result of the Data Breach, Plaintiffs Sauve and A.S. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Sauve and A.S. have a continuing interest in ensuring that Plaintiff Sauve's PII and Plaintiff A.S.'s PII and PHI, which upon information and belief remain in PowerSchool's possession, are protected and safeguarded from future data breaches.

i. GEORGIA PARENT JOHN RAWLS AND MINOR STUDENT C.R.

402. Plaintiff John Rawls ("Plaintiff Rawls") and his minor child C.R. ("Plaintiff C.R.") are citizens and residents of Georgia. At all relevant times, Plaintiff C.R. was a student of Buford Academy and previously Buford Elementary, which used PowerSchool's SIS. Plaintiff C.R. has been enrolled in the Buford Academy and previously Buford Elementary since Fall 2024 and Fall 2023 respectively. As a condition of Plaintiff C.R.'s enrollment, Plaintiff Rawls's PII and C.R.'s PII and PHI were input into PowerSchool's SIS.

403. Plaintiff C.R. received an email dated February 26, 2024, notifying Plaintiff C.R. of the Data Breach.

404. As a result of the Data Breach and as recommended in the Notice, Plaintiff Rawls made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor child's PII and PHI.

405. Plaintiff Rawls has spent significant time responding to the Data Breach on behalf of himself and Plaintiff C.R., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and time searching financial reports/bills for fraudulent charges, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Rawls suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiff C.R.'s PII and PHI.

406. PowerSchool was legally obligated to protect Plaintiffs Rawls and C.R.'s PII and PHI. Plaintiff Rawls would not have allowed his family's PII and PHI to be

shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

407. Thus, as a result of the Data Breach, Plaintiffs Rawls C.R. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Rawls C.R. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

j. GEORGIA PARENT KATHERINE STEWART AND MINOR STUDENT R.H.S.

408. Plaintiff Katherine Stewart ("Plaintiff Stewart") and her minor child R.H.S. ("Plaintiff R.H.S.") are citizens and residents of Georgia. At all relevant times, Plaintiff R.H.S. was a student at Fairyland Elementary School, which used PowerSchool's SIS. Plaintiff R.H.S. has been enrolled at Fairyland Elementary School since March 2023. As a condition of Plaintiff R.H.S.'s enrollment, Plaintiffs Stewart and R.H.S.'s PII and PHI were input into PowerSchool's SIS, including but not limited to Plaintiff R.H.S.'s date of birth, social security number, and medical information, Plaintiffs Stewart and R.H.S.'s home address and phone number, and Plaintiff Stewart's email address.

409. Plaintiff Stewart received an email from PowerSchool dated March 2, 2025, notifying her about the Data Breach.

410. As a result of the Data Breach and as recommended in the Notice, Plaintiff Stewart made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII and PHI.

411. Plaintiff Stewart has spent significant time responding to the Data Breach on behalf of herself and Plaintiff R.H.S., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will

continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Stewart has also spent significant time disputing unauthorized credit card charges and reporting and blocking spam emails. Plaintiff Stewart suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff R.H.S.'s PII and PHI.

412. PowerSchool was legally obligated to protect Plaintiffs Stewart and R.H.S.'s PII and PHI. Plaintiff Stewart would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

413. Thus, as a result of the Data Breach, Plaintiffs Stewart and R.H.S. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for Plaintiffs Stewart and R.H.S.'s lifetimes. Plaintiffs Stewart and R.H.S. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

k. IDAHO PARENT MARY LORENE MUCKELORY AND MINOR STUDENTS D.W.M. AND J.R.M.

414. Plaintiff Mary Lorene Muckelroy ("Plaintiff Muckelroy") and her minor children D.W.M. and J.R.M. ("Plaintiffs D.W.M. and J.R.M.") are citizens and residents of Idaho. At all relevant times, Plaintiffs D.W.M and J.R.M. were students at North Star Charter, which used PowerSchool's SIS. Plaintiffs D.W.M. and J.R.M. have been enrolled at North Star Charter since October 2018 and August 2018, respectively. As a condition of Plaintiffs D.W.M. and J.R.M.'s enrollment, Plaintiffs Muckelroy,

D.W.M., and J.R.M.'s PII were input into PowerSchool's SIS, including but not limited to their full names, addresses, dates of birth, emergency contact information, transportation arrangements (including whether the students ride the school bus), other household residents, D.W.M.'s need for an earplug for water-related school activities, and Plaintiff Muckelroy's place of employment and phone number.

415. Plaintiff Muckelroy received an email from North Star Charter dated January 13, 2025, notifying families of the Data Breach, followed by a second email on February 4, 2025, providing an update. She also received multiple emails from PowerSchool regarding the breach: on February 15, 2025, on behalf of J.R.W.; on March 2, 2025, on behalf of D.W.M.; and again on March 9, 2025, on behalf of J.R.W.

416. As a result of the Data Breach and as recommended in the Notice, Plaintiff Muckelroy made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII.

417. Plaintiff Muckelroy has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs D.W.M. and J.R.M., including enrolling in Experian IdentityWorks, and checking her financial statements, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Muckelroy suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs D.W.M. and J.R.M.'s PII.

418. PowerSchool was legally obligated to protect Plaintiffs Muckelroy, D.W.M. and J.R.M.'s PII. Plaintiff Muckelroy would not have allowed her family's PII to be shared with or accessible by PowerSchool if Plaintiff Muckelroy had known

PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

419. Thus, as a result of the Data Breach, Plaintiffs Muckelroy, D.W.M., and J.R.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Muckelroy, D.W.M., and J.R.M. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

l. ILLINOIS PARENT NICOLE COSENTINO AND MINOR STUDENT C.M.C.

420. Plaintiffs Nicole Cosentino ("Plaintiff Cosentino") and her minor child C.M.C. ("Plaintiff C.M.C.") are citizens and residents of Illinois. At all relevant times, Plaintiff C.M.C. was a student at Evergreen Elementary School, which used PowerSchool's SIS. Plaintiff C.M.C. has been enrolled at Evergreen Elementary School since August 2022. As a condition of Plaintiff C.M.C.'s enrollment, Plaintiff Cosentino's PII and Plaintiff C.M.C.'s PII and PHI was input into PowerSchool's SIS, including but not limited to Plaintiff C.M.C.'s date of birth and medical information, Plaintiffs Cosentino and C.M.C.'s home address and phone number, and Plaintiff Cosentino's email address.

421. Plaintiff Cosentino received an email dated March 3, 2025, notifying of the Data Breach.

422. As a result of the Data Breach and as recommended in the Notice, Plaintiff Cosentino made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and Plaintiff C.M.C.'s PII and PHI.

423. Plaintiff Cosentino has spent significant time responding to the Data Breach on behalf of herself and Plaintiff C.M.C, including addressing an extreme increase in spam communications, and will continue to spend valuable time she

otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Cosentino has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff C.M.C.'s PII and PHI.

424. PowerSchool was legally obligated to protect Plaintiffs Cosentino and C.M.C.'s PII and PHI. Plaintiff Cosentino would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

425. Thus, as a result of the Data Breach, Plaintiffs Cosentino and C.M.C. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Cosentino and C.M.C. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

m. ILLINOIS PARENT JILL STRELZIN AND MINOR STUDENTS J.S. AND R.S.

426. Plaintiffs Jill Strelzin ("Plaintiff Strelzin") and her minor children J.S. ("Plaintiff J.S.") and R.S. ("Plaintiff R.S.") are citizens and residents of Illinois. At all relevant times, Plaintiffs J.S. and R.S. were students at Glenbrook High School District 225, which used PowerSchool's SIS. Plaintiff J.S. has been enrolled at Glenbrook High School District 225 from August 2022 to present, and Plaintiff R.S. has been enrolled at Glenbrook High School District 225 from August 2024 to present. As a condition of Plaintiffs J.S. and R.S.'s enrollment as students at Glenbrook High School District 225, Plaintiffs Strelzin's PII and Plaintiffs J.S. and R.S.'s PII and PHI were input into PowerSchool's SIS to promote interoperability of educational services.

427. Plaintiff Strelzin received an email dated January 7, 2025, notifying Plaintiff Strelzin of the Data Breach.

428. As a result of the Data Breach and as recommended in the Notice, Plaintiff Strelzin made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

429. Plaintiff Strelzin has spent significant time, including searching through her credit card bills for fraudulent activity, responding to the Data Breach, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Strelzin suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach. Plaintiff Strelzin has increased concerns regarding the loss of her family's privacy, and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs J.S. and R.S.'s PII and PHI.

430. PowerSchool was legally obligated to protect Plaintiffs Strelzin, J.S., and R.S.'s PII and PHI. Plaintiff Strelzin would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

431. Thus, as a result of the Data Breach, Plaintiffs Strelzin, J.S., and R.S. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Strelzin, J.S., and R.S. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

n. ILLINOIS PARENT NICOLE VOLPERT AND MINOR STUDENT S.R.V.

432. Plaintiffs Nicole Volpert ("Plaintiff Volpert") and her minor child S.R.V. ("Plaintiff S.R.V.") are citizens and residents of Illinois. At all relevant times, Plaintiff S.R.V. was a student in the East Maine School District 63, which used PowerSchool's SIS. Plaintiff S.R.V. has been enrolled in the East Maine School District 63 since

August 2016. As a condition of Plaintiff S.R.V.'s enrollment, Plaintiffs Volpert and S.R.V.'s PII and PHI were inputted into PowerSchool's SIS, including but not limited to immunization records, addresses, birth certificates, health records, bills, her drivers' license, and Social Security Numbers.

433. Plaintiff Volpert received an email dated January 9, 2025, from East Maine School District 63, notifying Volpert about the Data Breach. On March 6, 2025, Plaintiff Volpert received notification from Powerschool regarding the Data Breach.

434. As a result of the Data Breach and as recommended in the Notice, Plaintiff Volpert made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII and PHI.

435. Plaintiff Volpert has spent time responding to the Data Breach on behalf of herself and Plaintiff S.R.V., including at least 5 hours addressing a large increase in spam calls and messages and monitoring her accounts that interfere with volunteer duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, childcare, and/or recreation. Plaintiff Volpert was notified by the IRS that someone tried to submit a fraudulent tax return in her name in 2025. Plaintiff Volpert suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff S.R.V.'s PII and PHI.

436. PowerSchool was legally obligated to protect Plaintiffs Volpert and S.R.V.'s PII and PHI. Plaintiff Volpert would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

437. Thus, as a result of the Data Breach, Plaintiffs Volpert and S.R.V. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Volpert and S.R.V. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

o. INDIANA PARENT AMANDA VOLTZ AND MINOR STUDENTS B.L.C. AND K.D.V.

438. Plaintiff Amanda Rachelle Voltz ("Plaintiff Voltz") and her minor children B.L.C. ("Plaintiff B.L.C.") and K.D.V. ("Plaintiff K.D.V.") are citizens and residents of Indiana. At all relevant times, Plaintiffs B.L.C. and K.D.V. were students in the Vincennes Community School Corp., which used PowerSchool's SIS. Plaintiffs B.L.C. and K.D.V. have been enrolled in the Vincennes Community School Corp. since August 3, 2017, and August 12, 2022, respectively. As a condition of Plaintiffs B.L.C. and K.D.V.'s enrollment, Plaintiffs Voltz, B.L.C., and K.D.V.'s PII, and Plaintiff K.D.V.'s PHI were input into PowerSchool's SIS, including but not limited to dates of birth, addresses, ethnicity, medical diagnosis, and gender identity.

439. Plaintiff Voltz received an email dated March 8, 2025, regarding B.L.C. and an email dated March 9, 2025, regarding K.D.V., notifying Voltz about the Data Breach.

440. As a result of the Data Breach and as recommended in the Notice, Plaintiff Voltz made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

441. Plaintiff Voltz has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs B.L.C. and K.D.V., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other

activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Voltz also received a fraudulent medical bill for K.D.V. and spent time addressing the fraudulent billing. Voltz suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs B.L.C. and K.D.V.'s PII and PHI.

442. PowerSchool was legally obligated to protect Plaintiffs Voltz, B.L.C., and K.D.V.'s PII and PHI. Plaintiff Voltz would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

443. Thus, as a result of the Data Breach, Plaintiffs Voltz, B.L.C., and K.D.V. have faced, and will continue to face, a present and continuing risk of fraud and identity theft their lifetimes. Plaintiffs Voltz, B.L.C., and K.D.V. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

p. IOWA PARENT KYLIE STOWE AND MINOR STUDENT Z.S.

444. Plaintiff Kylie Stowe ("Plaintiff Stowe") and her minor child Z.S. ("Plaintiff Z.S.") are citizens and residents of Iowa. At all relevant times, Plaintiff Z.S. was a student at Council Bluffs Community School District, which used PowerSchool's SIS. Plaintiff Z.S. has been enrolled in Council Bluffs Community School District since April or May of 2021. As a condition of Plaintiff Z.S.'s enrollment, Plaintiff Stowe's PII and Plaintiff Z.S.'s PII and PHI were input into PowerSchool's SIS.

445. Plaintiff Z.S. received an email from Council Bluffs Community School District dated January 9, 2025, notifying Plaintiff Z.S. of the Data Breach. They also received similar correspondence directly from PowerSchool on February 25, 2025.

446. As a result of the Data Breach and as recommended in the Notice, Plaintiff Stowe made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

447. Plaintiff Stowe has spent significant time responding to the Data Breach on behalf of herself and Plaintiff Z.S., which includes time spent verifying the legitimacy of the Notice of Data Breach, and monitoring her own and Plaintiff Z.S.'s information to ensure no fraudulent activity has occurred, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Stowe has experienced an increase in scam calls and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using Plaintiff Stowe's PII and Plaintiff Z.S.'s PII and PHI.

448. PowerSchool was legally obligated to protect Plaintiffs Stowe and Z.S.'s PII. Plaintiff Stowe would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

449. Thus, as a result of the Data Breach, Plaintiffs Stowe and Z.S. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Stowe and Z.S. have a continuing interest in ensuring that Plaintiff Stowe's PII and Plaintiff Z.S.'s PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

q. Kansas Parent Shanda Farquhar and Minor Student G.A.F.

450. Plaintiff Shanda Farquhar ("Plaintiff Farquhar") and her minor child G.A.F. (Plaintiff G.A.F.) are citizens and residents of Kansas. At all relevant times Plaintiff G.A.F. was a student at Wellsville High School, which used PowerSchool's SIS at all relevant times. As a condition of Plaintiff G.A.F.'s enrollment and receipt of educational services, Plaintiffs Farquhar and G.A.F.'s PII and PHI were input into PowerSchool's SIS to promote interoperability of educational services.

451. At all relevant times, Plaintiff G.A.F. was a student at Wellsville High School, which used PowerSchool's SIS; specifically, Plaintiff G.A.F. was enrolled in Wellsville High School from August 2022 until present. As a condition of Plaintiff G.A.F.'s enrollment as a student at Wellsville High School Plaintiffs Farquhar and G.A.F.'s PII and PHI were input into PowerSchool's SIS to promote interoperability of educational services, including but not limited to Plaintiffs Farquhar and G.A.F.'s birth dates, phone number, and address, and other information about Plaintiff G.A.F. in the possession of Wellsville High School, including PHI.

452. As a result of the Data Breach, Plaintiff Farquhar made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts. Since the Data Breach, Plaintiff Farquhar has had fraudulent purchases made on her Apple account.

453. Plaintiff Farquhar has spent significant time, including several hours of phone calls, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Farquhar suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over

the impact of cybercriminals accessing and using her and Plaintiff G.A.F.'s PII and PHI.

454. PowerSchool received Plaintiffs Farquhar and G.A.F.'s PII and PHI as a condition of Plaintiff G.A.F.'s enrollment in Wellsville High School from August 2022 to present. Upon information and belief, PowerSchool retained Plaintiffs Farquhar and G.A.F.'s PII and PHI as a result of Plaintiff G.A.F.'s active enrollment with Wellsville High School and likely still possesses Plaintiffs Farquhar and G.A.F.'s PII and PHI to this day. Plaintiff Farquhar reviewed and consented to forms that she believed included PowerSchool's privacy policies. Plaintiff Farquhar reasonably believed that PowerSchool would – indeed that PowerSchool was contractually and legally obligated to – protect Plaintiffs Farquhar and G.A.F.'s PII and PHI once it was provided to PowerSchool. Plaintiff Farquhar would not have provided Plaintiffs Farquhar and G.A.F.'s PII and PHI to PowerSchool if she had known PowerSchool would not adequately protect Plaintiffs Farquhar and G.A.F.'s PII and PHI, including by failing to implement and maintain sufficient data security safeguards to adequately protect Plaintiffs Farquhar and G.A.F.'s PII and PHI.

455. Plaintiffs Farquhar and G.A.F. suffered damages proximately caused by the Data Breach.

456. Thus, as a result of the Data Breach, Plaintiffs Farquhar and G.A.F. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Farquhar and G.A.F. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

r. LOUISIANA PARENT SCOTT GRECI AND MINOR STUDENT L.G.

457. Plaintiff Scott Greci ("Plaintiff Greci") and his minor child L.G. ("Plaintiff L.G.") are citizens and residents of Louisiana. At all relevant times, Plaintiff

L.G. was a student at Spanish Lakes Primary School, which used PowerSchool's SIS. Plaintiff L.G. was enrolled in the Ascension Parish Public Schools since at least August 2021. As a condition of Plaintiff L.G.'s enrollment as a student in Ascension Parish School District, Plaintiff Greci's PII and Plaintiff L.G.'s PII and PHI were input into PowerSchool's SIS, including but not limited to Plaintiff L.G.'s date of birth, social security number, Plaintiffs Greci and L.G.'s home address, and payment information for school lunches.

458. Plaintiff Greci received an email dated January 10, 2025, notifying Plaintiff Greci of the Data Breach.

459. As a result of the Data Breach and as recommended in the Notice, Plaintiff Greci made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor child's PII.

460. Plaintiff Greci has spent significant time responding to the Data Breach on behalf of Plaintiff L.G., including several hours of emails and phone calls, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Greci has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using Plaintiff Greci's PII and Plaintiff L.G.'s PII and PHI.

461. PowerSchool was legally obligated to protect Plaintiffs Greci and L.G.'s PII. Plaintiff Greci would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

462. Thus, as a result of the Data Breach, Plaintiffs Greci and L.G. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Greci and L.G. have a continuing interest in ensuring that their

PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

s. LOUISIANA PARENT TIFFANY HONORE AND MINOR STUDENT M.M.

463. Plaintiff Tiffany Honore ("Plaintiff Honore") and her minor child M.M. ("Plaintiff M.M.") are citizens and residents of Louisiana. At all relevant times, Plaintiff M.M. was a student at Edna Karr High School and previously ReNEW Dolores T. Aaron Academy, which used PowerSchool's SIS. Plaintiff M.M. has been enrolled in Edna Karr High School and previously ReNew Dolores T. Aaron Academy since August 2023 and July 2014 respectively. As a condition of Plaintiff M.M.'s enrollment, Plaintiff Honore's PII and M.M.'s PII and PHI were input into PowerSchool's SIS.

464. Plaintiff M.M. via Plaintiff Honore received an email dated February 14, 2025, notifying Plaintiff M.M. of the Data Breach.

465. As a result of the Data Breach and as recommended in the Notice, Plaintiff Honore made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect their own and their minor child's PII and PHI.

466. Plaintiff Honore, has spent significant time responding to the Data Breach on behalf of herself and Plaintiff M.M., including addressing a noticeable increase in spam calls and messages directed both to herself and M.M., and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Honore suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff M.M.'s PII and PHI.

467. PowerSchool was legally obligated to protect Plaintiffs Honore and M.M.'s PII. Plaintiff Honore would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

468. Thus, as a result of the Data Breach, Plaintiffs Honore and M.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Honore and M.M. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

t. MARYLAND PARENT ALYSHA NOBLE AND MINOR STUDENT R.J.S.

469. Alysha Noble ("Plaintiff Noble") and her minor child R.J.S. ("Plaintiff R.J.S.") are citizens and residents of the state of Maryland. At all relevant times, Plaintiff R.J.S. was a student at Broadford Elementary School in Garrett County Public School District, which used PowerSchool's SIS at all relevant times. Plaintiff R.J.S. was enrolled at Broadford Elementary School in Garrett County Public School District from September 2019 to present. As a condition of Plaintiff R.J.S.'s enrollment as a student at Broadford Elementary School in Garrett County Public School District, Plaintiffs Noble and R.J.S.'s PII was input into PowerSchool's SIS, including but not limited to Plaintiffs Noble and R.J.S.'s birth dates, phone number, and address, and other information about Plaintiff R.J.S. in the possession of Garrett County Public School District, including potentially PHI.

470. As a result of the Data Breach, Plaintiff Noble made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, monitoring her credit, and maintaining diligent review of her banking and other accounts. Since the Data Breach, Experian has notified Plaintiff Noble that her information has been listed on the dark web. She has had fraudulent purchases made

on her AT&T account. When she filed for unemployment benefits, she was notified that someone had already claimed Plaintiff R.J.S. as a dependent and had to provide proof that she was Plaintiff R.J.S.'s parent.

471. Plaintiff Noble has spent significant time responding to the Data Breach, including several hours of phone calls, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Noble suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her and Plaintiff R.J.S.'s PII.

472. PowerSchool was legally obligated to protect Plaintiffs Noble and R.J.S.'s PII. Plaintiff Noble would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

473. Thus, as a result of the Data Breach, Plaintiffs Noble and R.J.S. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Noble and R.J.S. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

u. MASSACHUSETTS PARENT JESSICA LEE ALLEN AND MINOR STUDENT C.A.

474. Plaintiff Jessica Lee Allen ("Plaintiff Allen") and her minor child C.A. ("Plaintiff C.A.") are citizens and residents of Massachusetts. At all relevant times, Plaintiff C.A. was a student at Granite Valley School in Monson County, Massachusetts, which used PowerSchool's SIS. Plaintiff C.A. has been enrolled at Granite Valley School since August 2020. As a condition of Plaintiff C.A.'s enrollment as a student at Granite Valley School, Plaintiff Allen's PII and Plaintiff C.A.'s PII and

PHI were input into PowerSchool's SIS, including but not limited to Plaintiff C.A.'s address, custody information, emergency contacts, medically protected information including doctor's name, health insurance carrier, medicines, and medical diagnoses, and, upon information and belief, additional information uploaded by the school without requesting or receiving consent from Plaintiff C.A.'s parents.

475. Plaintiff Allen received an email dated January 10, 2025, notifying "families and educators" of the Data Breach.

476. As a result of the Data Breach and as recommended in the Notice, Plaintiff Allen made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach reviewing PowerSchool's privacy policy, maintaining diligent review of her family's banking and other accounts, and seeking to protect her own PII and Plaintiff C.A.'s PII and PHI. Plaintiff Allen also purchased, at her own expense, credit monitoring services from Aura.

477. Plaintiff Allen has spent significant time, including several hours of phone calls, responding to the Data Breach on her own behalf and on behalf of Plaintiff C.A., and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Allen suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her own and Plaintiff C.A.'s privacy and potential further threats and damages over the impact of cybercriminals accessing and using Plaintiff Allen's PII and Plaintiff C.A.'s PII and PHI.

478. What's more, the school district, without requesting or receiving parental consent, uploaded Plaintiff C.A.'s school photo to PowerSchool, and, on information and belief, PowerSchool maintained records of Plaintiff C.A.'s exact classroom locations at any given time of the school day, as well as Plaintiff C.A.'s bus number and drop off/pick up times, all of which is visible in the school view of PowerSchool.

This poses a significant threat to Plaintiff C.A.'s physical safety and is of serious concern to Plaintiff Allen, particularly insofar as PowerSchool has continued to this day to have failed to inform Plaintiff Allen as to what specific data regarding Plaintiff C.A. has been breached.

479. PowerSchool was legally obligated to protect Plaintiffs Allen and C.A.'s PII and PHI. Plaintiff Allen would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

480. Thus, as a result of the Data Breach, Plaintiffs Allen and C.A. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Allen and C.A. have a continuing interest in ensuring that their PII and PHI, which, upon information and belief, remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

v. MASSACHUSETTS PARENT JENNAANN BERRY AND MINOR STUDENT G.B.

481. Plaintiff JennaAnn Berry ("Plaintiff Berry") and her minor child G.B. ("Plaintiff G.B.) are citizens and residents of Massachusetts. At all relevant times, Plaintiff G.B. was a student at Monson High School in Monson County, Massachusetts, which used PowerSchool's SIS. Plaintiff G.B. has been enrolled at Monson High School since August 2022. As a condition of Plaintiff G.B.'s enrollment as a student at Monson High School, Plaintiffs Berry's PII and Plaintiff G.B.'s PII and PHI were input into PowerSchool's SIS, including but not limited to Plaintiff G.B.'s address, custody information, emergency contacts, medically protected information including Plaintiff G.B.'s doctor's name, health insurance carrier, medicines, and medical diagnoses, and, upon information and belief, additional information uploaded by the school without requesting or receiving consent from Plaintiff G.B.'s parents.

482. Plaintiff Berry received an email dated January 10, 2025, notifying "families and educators" of the Data Breach.

483. As a result of the Data Breach and as recommended in the Notice, Plaintiff Berry made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, discussing the Data Breach with her sister and fellow plaintiff, Plaintiff Jessica Allen, reviewing PowerSchool's privacy policy, making phone calls, maintaining diligent review of her family's banking and other accounts, researching the Data Breach and seeking to protect her PII and Plaintiff G.B.'s PII and PHI.

484. Plaintiff Berry has spent significant time, including several hours of phone calls, online reviewing of accounts, and credit monitoring, responding to the Data Breach on her own behalf and on behalf of Plaintiff G.B., and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Berry suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further threats and damages over the impact of cybercriminals accessing and using her own and Plaintiff G.B.'s PII and PHI.

485. What's more, the school district, without requesting or receiving parental consent, uploaded Plaintiff G.B.'s school photo to PowerSchool, and, on information and belief, PowerSchool maintained records of Plaintiff G.B.'s exact classroom locations at any given time of the school day, as well as Plaintiff G.B.'s bus number and drop off/pick up times, all of which is visible in the school view of PowerSchool. This poses a significant threat to Plaintiff G.B.'s physical safety and is of serious concern to Plaintiff Berry, particularly insofar as PowerSchool has continued to this day to have failed to inform Plaintiff Berry as to what specific data regarding Plaintiff G.B. has been breached.

486. PowerSchool was legally obligated to protect Plaintiffs Berry and G.B.'s PII and PHI. Plaintiff Berry would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

487. Thus, as a result of the Data Breach, Plaintiffs Berry and G.B. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Berry and G.B. have a continuing interest in ensuring that their PII and PHI, which, upon information and belief, remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

w. MICHIGAN PARENT RUSHDA AFZAL AND MINOR STUDENTS Z.W. A.M.W. AND A.N.W.

488. Plaintiff Rushda Afzal ("Plaintiff Afzal") and her minor children Z.W. ("Plaintiff Z.W."), A.M.W. ("Plaintiff A.M.W."), and A.N.W. ("Plaintiff A.N.W.) are citizens and residents of Michigan. At all relevant times, Plaintiffs Z.W., A.M.W., and A.N.W. were students of Crescent Academy International, located in Canton, Michigan, which used PowerSchool's SIS. Plaintiffs Z.W., A.M.W., and A.N.W. have been enrolled in Crescent Academy International since August 2016. As a condition of Plaintiffs Z.W., A.M.W., and A.N.W.'s enrollment as students at Crescent Academy International, Plaintiff Afzal's PII and Plaintiffs Z.W., A.M.W., and A.N.W.'s PII and PHI were input into PowerSchool's SIS to promote interoperability of educational services, including but not limited to Plaintiffs Z.W., A.M.W., and A.N.W.'s enrollment records and Plaintiff Azfal's personal phone number.

489. On January 7, 2025, Plaintiffs Afzal received an email from Crescent Academy International, notifying her about the Data Breach.

490. As a result of the Data Breach and as recommended in the Notice, Plaintiff Afzal made reasonable efforts to mitigate the impact of the Data Breach, including, but

not limited to, researching the Data Breach and seeking to protect her own PII and Plaintiffs Z.W., A.M.W., and A.N.W.'s PII and PHI.

491. Plaintiff Afzal has spent significant time, including multiple hours monitoring her accounts for fraudulent changes and addressing an influx of fraudulent phone calls that interfere with work duties and personal time, responding to the Data Breach on behalf of herself and Plaintiffs Z.W., A.M.W., and A.N.W., and will continue to spend valuable time she otherwise would have been spent on other activities, including, but not limited to, work, childcare, and recreation. Plaintiff Afzal suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs Z.W., A.M.W., and A.N.W.'s PII and PHI.

492. PowerSchool was legally obligated to protect Plaintiffs Afzal, Z.W., A.M.W., and A.N.W.'s PII. Plaintiff Afzal would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

493. Thus, as a result of the Data Breach, Plaintiffs Afzal, Z.W., A.M.W., and A.N.W. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Afzal, Z.W., A.M.W., and A.N.W. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

x. MICHIGAN PARENT RATIB HABBAL AND MINOR STUDENT L.H.

494. Plaintiff Ratib Habbal ("Plaintiff Habbal") and his minor child L.H. ("Plaintiff L.H.") are citizens and residents of Michigan. At all relevant times, Plaintiff L.H. was a student of Crescent Academy International, located in Canton, Michigan,

which used PowerSchool's SIS. Plaintiff L.H. has been enrolled in Crescent Academy International since August 2015. As a condition of Plaintiff L.H.'s enrollment as a student at Crescent Academy International, Plaintiffs Habbal and L.H.'s PII was input into PowerSchool's SIS.

495. In January 2025, Plaintiff L.H. received an email from Crescent Academy International, notifying Plaintiff L.H. about the Data Breach.

496. As a result of the Data Breach and as recommended in the Notice, Plaintiff Habbal made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his and his minor child's PII.

497. Plaintiff Habbal has spent significant time responding to the Data Breach on behalf of himself and Plaintiff L.H. and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and recreation. Plaintiff Habbal suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his and Plaintiff L.H.'s PII.

498. PowerSchool was legally obligated to protect Plaintiffs Habbal and L.H.'s PII once it was provided to PowerSchool. Plaintiff Habbal would not have allowed her family's PII to be shared with or accessibly by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

499. Thus, as a result of the Data Breach, Plaintiffs Habbal and L.H. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Habbal and L.H. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

y. MICHIGAN PARENT TRISHA NADEAU AND MINOR STUDENTS G.O.E. AND J.C.E.

500. Plaintiffs Trisha Nadeau ("Plaintiff Nadeau") and her minor children G.O.E. and J.C.E. ("Plaintiffs G.O.E. and J.C.E.") are citizens and residents of Michigan. At all relevant times, Plaintiffs G.O.E. and J.C.E. were students at Dansville Elementary School, which used PowerSchool's SIS. Plaintiffs G.O.E. and J.C.E. have been enrolled at Dansville Elementary School since August 2019. As a condition of Plaintiffs G.O.E. and J.C.E.'s enrollment, Plaintiffs Nadeau, G.O.E., and J.C.E.'s PII were input into PowerSchool's SIS, including but not limited to dates of birth, Social Security Numbers, addresses, phone numbers, and financial information.

501. Plaintiff Nadeau received emails dated February 27, 2025, and March 3, 2025, notifying her of the Data Breach.

502. As a result of the Data Breach and as recommended in the Notice, Plaintiff Nadeau made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII.

503. Plaintiff Nadeau has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs G.O.E. and J.C.E., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Her minor children have also been receiving spam calls and texts since the Data Breach. Plaintiff Nadeau has suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has also experienced fraudulent charges in excess of $4,000 that have negatively impacted her credit score. Plaintiff Nadeau has increased concerns regarding the loss of her family's privacy and potential

further damages over the impact of cybercriminals accessing and using her own and Plaintiffs G.O.E. and J.C.E.'s PII.

504. PowerSchool was legally obligated to protect Plaintiffs Nadeau, G.O.E., and J.C.E.'s PII. Plaintiff Nadeau would not have allowed her family's PII to be shared with or accessible by PowerSchool if Plaintiff Nadeau had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

505. Thus, as a result of the Data Breach, Plaintiffs Nadeau, G.O.E., and J.C.E. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Nadea, G.O.E., and J.C.E. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

z. MINNESOTA PARENT AMY HAUSER AND MINOR STUDENT J.H.

506. Plaintiffs Amy Hauser ("Plaintiff Hauser") and her minor child J.H. ("Plaintiff J.H.") are citizens and residents of Minnesota. At all relevant times, Plaintiff J.H. was a student in the Caledonia Independent School District, which used PowerSchool's SIS. Plaintiff J.H. has been enrolled at School since Month 2019. As a condition of Plaintiff J.H.'s enrollment as a student in Caledonia Independent School District, Plaintiffs Hauser and J.H.'s PII and PHI were input into PowerSchool's SIS, including but not limited to contact and medical information.

507. Plaintiff Hauser received an email dated January 10, 2025, notifying her of the Data Breach.

508. As a result of the Data Breach and as recommended in the Notice, Plaintiff Hauser made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII and PHI.

509. Plaintiff Hauser has spent significant time, including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, responding to the Data Breach on behalf of her and Plaintiff J.H., and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Hauser also received bills from two different credit cards that were fraudulently opened in her name. Plaintiff Hauser suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff J.H.'s PII.

510. PowerSchool was legally obligated to protect Plaintiffs Hauser and J.H.'s PII and PHI. Plaintiff Hauser would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

511. Thus, as a result of the Data Breach, Plaintiffs Hauser and J.H. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Hauser and J.H. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

aa. MISSISSIPPI PARENT KATHEY HENRY AND MINOR STUDENTS T.M.H. AND T.T.H.

512. Plaintiff Kathey Henry ("Plaintiff Henry") and her minor children T.M.H. ("Plaintiff T.M.H.") and T.T.H. ("Plaintiff T.T.H.") are citizens and residents of Shubuta, Mississippi. At all relevant times, Plaintiffs T.M.H. and T.T.H. were students at Wayne Central School in Waynesboro, Mississippi, which used PowerSchool's SIS at all relevant times. Plaintiffs T.M.H. and T.T.H. were enrolled in Wayne Central School from August 2023 until the present. As a condition of Plaintiffs T.M.H. and

T.T.H.'s enrollment, Plaintiff Henry's PII and her children's PII and PHI were input into PowerSchool's SIS.

513. Plaintiff Henry received two emails dated February 14, 2025, notifying Plaintiff Henry of the Data Breach.

514. As a result of the Data Breach and as recommended in the Notice, Plaintiff Henry made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, maintaining diligent review of her family's banking and other accounts, and seeking to protect her own and her minor children's PII and PHI.

515. Plaintiff Henry has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs T.M.H. and T.T.H., including addressing a noticeable increase in spam calls and messages, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Henry has been receiving emails and bills about a Geek Squad account that she did not sign up for and a PayPal account that is not her PayPal account. Also, Plaintiff's husband had to get a new bank card because someone used his debit card, and it was not him. Plaintiff Henry suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs T.M.H. and T.T.H.'s PII and PHI.

516. PowerSchool was legally obligated to protect Plaintiffs Henry, T.M.H., and T.T.H's PII and PHI. Plaintiff Henry would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

517. Thus, as a result of the Data Breach, Plaintiff Henry, T.M.H., and T.T.H have faced, and will continue to face, a present and continuing risk of fraud and identity

theft for their lifetimes. Plaintiff Henry, T.M.H., and T.T.H have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

bb. MISSOURI PARENT OF FORMER STUDENT KRISTI KINGERY-ISLAS

518. Plaintiff Kristi Kingery-Islas ("Plaintiff Kingery-Islas") is a citizen and current resident of Missouri. At all relevant times, Plaintiff Kingery-Islas was the parent of a student at Liberty Public Schools in Liberty, Missouri, which used PowerSchool's SIS. Plaintiff Kingery-Islas' child was enrolled at Liberty Public Schools from August 2003 until May 2020. As a condition of Plaintiff Kingery-Islas's child's enrollment, Plaintiff Kingery-Islas's PII was input into PowerSchool's SIS, including but not limited to her home address, email, and phone numbers.

519. As a result of the Data Breach, Plaintiff Kingery-Islas made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

520. Plaintiff Kingery-Islas has spent significant time responding to the Data Breach, including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Kingery-Islas suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

521. PowerSchool was legally obligated to protect Plaintiff Kingery-Islas's PII. Plaintiff Kingery-Islas would not have allowed her PII to be shared with or accessible

by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

522. Thus, as a result of the Data Breach, Plaintiff Kingery-Islas has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Kingery-Islas has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

cc. MISSOURI PLAINTIFF TORRIE MAYFEILD AND MINOR STUDENT A.M.

523. Plaintiff Torrie Mayfeild ("Plaintiff Mayfeild") and her minor child A.M. (Plaintiff A.M.) are citizens and residents of Missouri. At all relevant times, Plaintiff A.M. was a student of Virtual Prep Academy of Missouri, which used PowerSchool's SIS. Plaintiff A.M. has been enrolled in Virtual Prep Academy of Missouri since August of 2024. As a condition of Plaintiff A.M. enrollment, Plaintiffs Mayfeild and A.M.'s PII was input into PowerSchool's SIS.

524. Plaintiff Mayfeild received an email dated January 10, 2025, notifying Plaintiff Mayfeild of the Data Breach.

525. As a result of the Data Breach and as recommended in the Notice, Plaintiff Mayfeild made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

526. Plaintiff Mayfeild has spent significant time responding to the Data Breach on behalf of herself and Plaintiff A.M., including spending time on the phone, reviewing her financial and credit monitoring accounts, and addressing an increase in spam and phishing calls, emails, and texts. Plaintiff Mayfeild will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Mayfeild suffered lost time,

annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and A.M.'s PII.

527. PowerSchool was legally obligated to protect Plaintiffs Mayfeild and A.M.'s PII. Plaintiff Mayfeild would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

528. Thus, as a result of the Data Breach, Plaintiffs Mayfeild and A.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Mayfeild and A.M. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

dd. MONTANA PARENT KATHLEEN HOLM AND MINOR STUDENTS P.P. AND R.P.

529. Plaintiff Kathleen Holm ("Plaintiff Holm") and her minor children P.P. ("Plaintiff P.P.") and R.P. ("Plaintiff R.P.") are citizens and residents of Big Fork, Montana. At all relevant times, Plaintiffs P.P. and R.P. were students at Big Fork Elementary in Big Fork, Montana, which used PowerSchool's SIS. Plaintiffs P.P. and R.P. were enrolled in Big Fork Elementary from August 2024 until June 2025. As a condition of Plaintiffs P.P. and R.P.'s enrollment, Plaintiff Holm's PII and Plaintiffs P.P. and R.P.'s PII and PHI were input into PowerSchool's SIS.

530. Plaintiff Holm received an email in Spring 2025, notifying Plaintiff Holm of the Data Breach.

531. As a result of the Data Breach and as recommended in the Notice, Plaintiff Holm made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, maintaining diligent review of the family's

banking and other accounts, and seeking to protect her own and her minor children's PII and PHI.

532. Plaintiff Holm has spent significant time responding to the Data Breach on her own behalf and on behalf of Plaintiffs P.P. and R.P. and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Holm suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs P.P. and R.P.'s PII and PHI.

533. PowerSchool was legally obligated to protect Plaintiffs Holm, P.P., and R.P.'s PII and PHI. Plaintiff Holm would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

534. Thus, as a result of the Data Breach, Plaintiffs Holm, P.P., and R.P. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Holm, P.P., and R.P. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

ee. NEW HAMPSHIRE PARENT SERENE BAVIS AND MINOR STUDENT S.W.

535. Plaintiff Serene Bavis ("Plaintiff Bavis") and her minor child S.W. ("Plaintiff S.W.") are citizens and residents of Woodsville, New Hampshire. At all relevant times, Plaintiff S.W. was a student at Woodsville Elementary School in Woodsville, New Hampshire, which used PowerSchool's SIS. Plaintiff S.W. was enrolled in Woodsville Elementary School from August 2024 until June 2025. As a

condition of Plaintiff S.W.'s enrollment, Plaintiff Bavis' PII and Plaintiff S.W.'s PII and PHI were input into PowerSchool's SIS.

536. Plaintiff Bavis received an email on February 15, 2025, notifying Plaintiff Bavis that of the Data Breach.

537. As a result of the Data Breach and as recommended in the Notice, Plaintiff Bavis made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her family's banking and other accounts, and seeking to protect her own and her minor child's PII and PHI.

538. Plaintiff Bavis has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Bavis suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her and Plaintiff S.W.'s PII and PHI.

539. PowerSchool was legally obligated to protect Plaintiffs Bavis and Child S.W.'s PII and PHI. Plaintiff Bavis would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

540. Thus, as a result of the Data Breach, Plaintiffs Bavis and S.W. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Bavis and S.W. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

ff. NEW JERSEY PARENT MELISSA GIFFORD AND MINOR STUDENTS J.M., C.M., AND J.S.M.

541. Plaintiff Melissa Gifford ("Plaintiff Gifford") and her minor children J.R.M. ("Plaintiff J.R.M."), C.A.M. ("Plaintiff C.A.M."), and J.S.M ("Plaintiff J.S.M") are citizens and residents of New Jersey. At all relevant times, Plaintiffs J.R.M., C.A.M., and J.S.M. were students in the Commercial Township School District in Port Norris, New Jersey, which used PowerSchool's SIS. Plaintiffs J.R.M., C.A.M., and J.S.M. have been enrolled in the district since approximately April 2019, December 2021 and September 2022 respectively. As a condition of Plaintiffs J.R.M., C.A.M., and J.S.M.'s enrollment, Plaintiffs Gifford, J.R.M., C.A.M., and J.S.M.'s PII were input into PowerSchool's SIS, including but not limited to the minor children's dates of birth, the family's address and phone number, and Plaintiff Gifford's email address.

542. Plaintiff Gifford received an email dated February 17, 2025, notifying her of the Data Breach. She received additional emails on or around February 14 and 24, 2025.

543. As a result of the Data Breach and as recommended in the Notice, Plaintiff Gifford made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII.

544. Plaintiff Gifford has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs J.R.M., C.A.M., and J.S.M., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work, childcare, and/or recreation. Subsequent to the Data Breach and signing up for an account with the credit monitoring service Experian, Plaintiff Gifford received a notification that her data was found on the dark web. Plaintiff Gifford suffered lost time, annoyance, interference, emotional

distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs J.R.M., C.A.M., and J.S.M.'s PII.

545. PowerSchool was legally obligated to protect Plaintiffs Gifford, J.R.M., C.A.M., and J.S.M.'s PII. Plaintiff Gifford would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

546. Thus, as a result of the Data Breach, Plaintiffs Gifford, J.R.M., C.A.M., and J.S.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Gifford, J.R.M., C.A.M., and J.S.M. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

gg. NEW JERSEY PARENT SAKINAH ARDINE KNOTT AND MINOR STUDENTS M.M.W., D.J.P., AND I.M.W.

547. Plaintiffs Sakinah Ardine Knott ("Plaintiff Knott") and her minor children M.M.W. ("Plaintiff M.M.W."), D.J.P. ("Plaintiff D.J.P."), and I.M.W. ("Plaintiff I.M.W.") are citizens and residents of New Jersey. At all relevant times, Plaintiffs M.M.W., D.J.P., and I.M.W. were students at Barringer High School and New Collegiate Academy in Newark, New Jersey, both of which used PowerSchool's SIS. Plaintiff M.M.W has been enrolled at Barringer High School since January 2025. Prior to that, Plaintiff M.M.W. was enrolled at New Collegiate Academy beginning in August 2023. Plaintiff D.J.P. has been enrolled at Barringer High School since January 2025. Prior to that, Plaintiff D.J.P. was enrolled at New Collegiate Academy beginning in August 2023. Plaintiff I.M.W. has been enrolled at Barringer High School since

September 2024. As a condition of Plaintiffs M.M.W., D.J.P., and I.M.W.'s enrollment as students at Barringer High School, Plaintiffs Knott, M.M.W., D.J.P., and I.M.W.'s PII and PHI were input into PowerSchool's SIS, including but not limited to addresses, phone numbers, names, medical information, and additional data input by the school.

548. Plaintiff Knott received an email dated March 6, 2025, notifying her about the Data Breach.

549. As a result of the Data Breach and as recommended in the Notice, Plaintiff Knott made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

550. Plaintiff Knott has spent significant time, including addressing a noticeable increase in spam calls, text messages, and emails that interfere with work duties and personal time, responding to the Data Breach on behalf of herself and Plaintiffs M.M.W., D.J.P., and I.M.W., and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Knott suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs M.M.W., D.J.P., and I.M.W.'s PII and PHI.

551. PowerSchool was legally obligated to protect Plaintiffs Knott, M.M.W., D.J.P., and I.M.W.'s PII and PHI. Plaintiff Knott would not have allowed Plaintiffs Knott, M.M.W., D.J.P., and I.M.W.'s PII and PHI to be shared with or accessible by PowerSchool if Plaintiff Knott had known PowerSchool would not maintain sufficient data security safeguards to adequately protect Plaintiffs Knott, M.M.W., D.J.P., and I.M.W.'s PII and PHI.

552. Thus, as a result of the Data Breach, Plaintiffs Knott, M.M.W., D.J.P., and I.M.W. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for Plaintiffs Knott, M.M.W., D.J.P., and I.M.W.'s lifetimes. Plaintiffs Knott, M.M.W., D.J.P., and I.M.W. have a continuing interest in ensuring that Plaintiffs Knott, M.M.W., D.J.P., and I.M.W.'s PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

hh. NEW YORK PARENT PATRICK BOWLER AND MINOR STUDENTS J.B. AND M.B.

553. Plaintiff Patrick Bowler ("Plaintiff Bowler") and his minor children J.B. ("Plaintiff J.B.") and M.B. ("Plaintiff M.B.") are citizens and residents of New York. At all relevant times, Plaintiffs J.B. and M.B. were students at Lynbrook High School and Lynbrook Middle School, respectively, which used PowerSchool's SIS. Plaintiff J.B. has been enrolled at Lynbrook High School since at least August 2024 and Plaintiff M.B. has been enrolled at Lynbrook Middle School since at least August 2024. As a condition of Plaintiffs J.B. and M.B.'s enrollment, Plaintiffs Bowler, J.B. and M.B.'s PII were input into PowerSchool's SIS.

554. Plaintiff Bowler was notified of the Data Breach in or around January 2025.

555. As a result of the Data Breach and as recommended in the Notice, Plaintiff Bowler made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor child's PII.

556. Plaintiff Bowler has spent significant time responding to the Data Breach on behalf of himself and Plaintiff J.B. and M.B., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time s/he otherwise would have spent on other

activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Bowler suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiff J.B. and M.B.'s PII.

557. PowerSchool was legally obligated to protect Plaintiffs Bowler and J.B. and M.B.'s PII. Plaintiff Bowler would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

558. Thus, as a result of the Data Breach, Plaintiffs Bowler and J.B. and M.B. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Bowler and J.B. and M.B. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

ii. NEW YORK PARENT JENNIFER CECILIA HARRELL AND MINOR STUDENT J.E.H.

559. Plaintiffs Jennifer Cecilia Harrell ("Plaintiff Harrell") and her minor child J.E.H. ("Plaintiff J.E.H.") are citizens and residents of New York. At all relevant times, Plaintiff J.E.H. was a student in the Franklin Central School District, which used PowerSchool's SIS. Plaintiff J.E.H. has been enrolled in the Franklin Central School District since September 2019. As a condition of Plaintiff J.E.H.'s enrollment, Plaintiffs Harrell and J.E.H.'s PII was input into PowerSchool's SIS.

560. Plaintiff Harrell received an email dated February 15, 2025, notifying Harrell about the Data Breach.

561. As a result of the Data Breach and as recommended in the Notice, Plaintiff Harrell made reasonable efforts to mitigate the impact of the Data Breach, including,

but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

562. Plaintiff Harrell has spent significant time responding to the Data Breach on behalf of herself and Plaintiff J.E.H., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Subsequent to the Data Breach, Plaintiff Harrell experienced unauthorized attempt to open a credit card with her information, which still shows up on her credit report, another instance of attempted identity fraud and was required to close another card as a result. Her information is also on the dark web. Plaintiff Harrell suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff J.E.H.'s PII.

563. PowerSchool was legally obligated to protect Plaintiffs Harrell and J.E.H.'s PII. Plaintiff Harrell would not have allowed her family's PII to be shared with or accessible by PowerSchool if Plaintiff Harrell had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

564. Thus, as a result of the Data Breach, Plaintiffs Harrell and J.E.H. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Harrell and J.E.H. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

jj. NORTH CAROLINA PARENT KRISTIN ECKART AND MINOR STUDENTS J.E. AND T.E.

565. Plaintiff Kristin Eckart ("Plaintiff Eckart") and her minor children J.E. ("Plaintiff J.E.") and T.E. ("Plaintiff T.E.") are citizens and residents of North Carolina.

At all relevant times, Plaintiffs J.E. and T.E. were students at Winston-Salem/Forsyth County School District, which used PowerSchool's SIS. Plaintiff J.E. has been enrolled in the Winston-Salem/Forsyth County School District since August 2017 and Plaintiff T.E. was enrolled in the Winston-Salem/Forsyth County School District from August 2016 to December 2022. As a condition of Plaintiffs J.E. and T.E.'s enrollment as students at Winston-Salem/Forsyth County School District, Plaintiff Eckart's PII and Plaintiffs J.E. and T.E.'s PII and PHI were input into PowerSchool's SIS.

566. Plaintiff Eckart received an email dated January 8, 2025, notifying "families and staff" of the Data Breach.

567. As a result of the Data Breach and as recommended in the Notice, Plaintiff Eckart made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

568. Plaintiff Eckart has spent significant time, including spending time reviewing and securing financial accounts and otherwise responding to the Data Breach on behalf of herself and Plaintiffs J.E. and T.E. and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Eckart suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs J.E. and T.E.'s PII and PHI.

569. PowerSchool was legally obligated to protect Plaintiffs Eckart, J.E., and T.E.'s PII and PHI. Plaintiff Eckart would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

570. As a result of the Data Breach, Plaintiffs Eckart, J.E., and T.E. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Eckart, J.E., and T.E. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

kk. NORTH CAROLINA (GEORGIA) PARENT JESSICA PATRICK TAYLOR AND MINOR STUDENTS J.O.P. AND N.O.T.

571. Plaintiff Jessica Patrick Taylor ("Plaintiff Taylor") and her minor children, J.O.P. ("Plaintiff J.O.P.") and N.O.T. ("Plaintiff N.O.T."), are citizens and residents of North Carolina. Plaintiff J.O.P. was enrolled at Rice Creek School in Georgia from August 2022 to June 2023 and Robert Groves High School in Georgia from August 2023 to October 2023, and Plaintiff N.O.T. was enrolled at Rice Creek School in Georgia from August 2022 to November 2023. Both schools used PowerSchool's SIS. As a condition of their enrollment, Plaintiffs Taylor, J.O.P., and N.O.T.'s PII were input into PowerSchool's SIS, including but not limited to addresses, phone numbers, names, birth certificates, and other data input by the schools.

572. Plaintiff J.O.P. has been enrolled at Orange High School in North Carolina since October 2023, and Plaintiff N.O.T. has been enrolled at Spring Valley Elementary School in North Carolina since August 2024. Plaintiff N.O.T. was additionally enrolled at Oak Grove School in North Carolina from November 2023 to June 2024. All three schools also use PowerSchool's SIS. As a condition of their enrollment, additional PII of Plaintiffs Taylor, J.O.P., and N.O.T. was input into PowerSchool's SIS.

573. Plaintiff Taylor first received notice of the Data Breach in an email dated February 11, 2025, from the schools in Georgia. She later received a second notice in an email dated May 7, 2025, from the schools in North Carolina.

574. As a result of the Data Breach and as recommended in the Notice, Plaintiff Taylor made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII.

575. Plaintiff Taylor has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs J.O.P. and N.O.T., including addressing a noticeable increase in spam calls, text messages, and emails that interfere with work duties and personal time, and Plaintiff Taylor will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Taylor suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs J.O.P. and N.O.T.'s PII.

576. PowerSchool was legally obligated to protect Plaintiffs Taylor, J.O.P. and N.O.T.'s PII. Plaintiff Taylor would not have allowed her family's PII to be shared with or accessible by PowerSchool if Plaintiff Taylor had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

577. As a result of the Data Breach, Plaintiffs Taylor, J.O.P. and N.O.T. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Taylor, J.O.P. and N.O.T. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

ll. NORTH DAKOTA PARENT MARIAH JENE MARTYN AND MINOR STUDENT L.M.A.

578. Plaintiffs Mariah Jene Martyn ("Plaintiff Martyn") and her minor child L.M.A. ("Plaintiff L.M.A.") are citizens and residents of North Dakota. At all relevant

times, Plaintiff L.M.A. was a student in the Grand Forks School District, which used PowerSchool's SIS. Plaintiff L.M.A. was enrolled in the Grand Forks School District from August 2019 to November 2020. As a condition of Plaintiff L.M.A.'s enrollment, Plaintiffs Martyn and L.M.A.'s PII and PHI were input into PowerSchool's SIS, including but not limited to medical history, addresses, and Social Security Numbers.

579. Plaintiff Martyn received an email dated May 7, 2025, notifying her about the Data Breach.

580. As a result of the Data Breach and as recommended in the Notice, Plaintiff Martyn made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII and PHI.

581. Plaintiff Martyn has spent significant time responding to the Data Breach on behalf of herself and Plaintiff L.M.A., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Martyn experienced a third party opening an AT&T phone line using her child's Social Security Number, which required additional time to address, including presenting to the store to have them flag the phone line as fraudulent. Plaintiff Martyn suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff L.M.A.'s PII and PHI.

582. PowerSchool was legally obligated to protect Plaintiffs Martyn and L.M.A.'s PII and PHI. Plaintiff Martyn would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if Plaintiff Martyn had known

PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

mm. OHIO PARENT ANDREW COOK AND MINOR STUDENTS A.C. AND C.C.

583. Plaintiff Andrew Cook ("Plaintiff Cook") and his two minor children A.C. ("Plaintiff A.C.") and C.C. ("Plaintiff C.C.") are citizens and residents of Ohio. At all relevant times, Plaintiffs A.C. and C.C. were students at Parkside Elementary School of Solon School District, which used PowerSchool's SIS. Plaintiff A.C. has been enrolled in the Parkside Elementary School since August 2021, and Plaintiff C.C. has been enrolled at Parkside Elementary School since August 2024. As a condition of Plaintiffs A.C. and C.C.'s enrollment as students at Parkside Elementary School, Plaintiff Cook's PII and Plaintiffs A.C. and C.C.'s PII and PHI, including medical records related to Plaintiff A.C.'s disability and Individualized Education Plan, were input into PowerSchool's SIS.

584. Plaintiffs A.C. and C.C. received emails dated January 10, 2025, notifying Plaintiffs A.C. and C.C. of the Data Breach.

585. As a result of the Data Breach and as recommended in the Notice, Plaintiff Cook made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor children's PII.

586. Plaintiff Cook has spent significant time responding to the Data Breach on behalf of himself and Plaintiffs A.C. and C.C. and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Cook suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further

damages over the impact of cybercriminals accessing and using his own and Plaintiffs A.C. and C.C.'s PII and PHI.

587. PowerSchool was legally obligated to protect Plaintiffs Cook, A.C., and C.C.'s PII and PHI. Plaintiff Cook would not have allowed his family's PII and PHI to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

588. As a result of the Data Breach, Plaintiffs Cook, A.C., and C.C. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Cook, A.C., and C.C. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

nn. OREGON PARENT CARA LEWIS AND MINOR STUDENTS A.L. AND M.L.

589. Plaintiff Cara Lewis ("Plaintiff Lewis") and her minor children A.L. ("Plaintiff A.L.") and M.L. ("Plaintiff M.L.") are citizens and residents of Oregon. At all relevant times, Plaintiffs A.L. and M.L. were students at Oregon Charter Academy, which used PowerSchool's SIS. Plaintiffs A.L. and M.L. have both been enrolled in the Oregon Charter Academy since September 2017. As a condition of Plaintiffs A.L. and M.L.'s enrollment, Plaintiffs Lewis, A.L. and M.L.'s PII were input into PowerSchool's SIS.

590. Plaintiffs Lewis, A.L., and M.L. received an email dated January 13, 2025, notifying Plaintiffs Lewis, A.L., and M.L. of the Data Breach.

591. As a result of the Data Breach and as recommended in the Notice, Plaintiff Lewis made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and Plaintiffs A.L. and M.L.'s PII.

592. Plaintiff Lewis spent significant time responding to the Data Breach on behalf of herself and Plaintiffs A.L. and M.L., including dealing with an increase in spam and phishing emails, spending time on phone calls and emails, and reviewing financial accounts, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Lewis suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using Plaintiffs Lewis, A.L., and M.L.'s PII.

593. PowerSchool was legally obligated to protect Plaintiffs Lewis, A.L., and M.L.'s PII. Plaintiff Lewis would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

594. Thus, as a result of the Data Breach, Plaintiffs Lewis, A.L., and M.L. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Lewis, A.L., and M.L. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

oo. PENNSYLVANIA PARENT FRANK JOHN TRZCINSKI AND MINOR STUDENTS E.T. AND S.T.

595. Plaintiffs Frank John Trzcinski ("Plaintiff Trzcinski") and his minor children E.T. ("Plaintiff E.T."), and S.T. ("Plaintiff S.T."), are citizens and residents of Pennsylvania. At all relevant times, Plaintiff E.T. was a student at Dingman Delaware Middle School and Plaintiff S.T. was a student at Dingman Delaware Primary School, both of which used PowerSchool's SIS. Plaintiff E.T. has been enrolled at Dingman Delaware Middle School since August 2024. Plaintiff S.T. has been enrolled at Dingman Delaware Primary School since August 2024. As a condition of Plaintiff's

children E.T. and S.T.'s enrollment, Plaintiffs Trzcinski, E.T. and S.T.'s PII were input into PowerSchool's SIS, including but not limited to addresses, phone numbers, names, social security numbers, and additional data input by the schools.

596. Plaintiff Trzcinski received an email dated March 1, 2025, notifying him of the Data Breach.

597. As a result of the Data Breach and as recommended in the Notice, Plaintiff Trzcinski made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor children's PII.

598. Plaintiff Trzcinski has spent significant time responding to the Data Breach on behalf of himself and Plaintiffs E.T. and S.T., including addressing a noticeable increase in spam calls, text messages, and emails that interfere with work duties and personal time, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Trzcinski has received confirmation that, since the breach, his son Plaintiff E.T. has had his social security number used by other parties. Plaintiff Trzcinski suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiffs E.T. and S.T.'s PII.

599. PowerSchool was legally obligated to protect Plaintiffs Trzcinski, E.T. and S.T.'s PII. Plaintiff Trzcinski would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their's PII.

600. As a result of the Data Breach, Plaintiffs Trzcinski, E.T. and S.T. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Trzcinski, E.T. and S.T. have a continuing interest in

ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

pp. SOUTH CAROLINA PARENT NICOLE DRENNEN AND MINOR STUDENTS G.D. AND Q.D.

601. Plaintiff Nicole Ann Drennen ("Plaintiff Drennen") and her minor children G.D. ("Plaintiff G.D.") and Q.D. ("Plaintiff Q.D.") are citizens and residents of South Carolina. At all relevant times, Plaintiffs G.D. and Q.D. were students in the Charleston School District, which used PowerSchool's SIS. Plaintiff G.D. was enrolled in Laurel Hill Primary School from August 2021 until the present, and Plaintiff Q.D. was enrolled in Laurel Hill Primary School from August 2022 until the present. As a condition of Plaintiffs G.D. and Q.D. enrollment at Laurel Hill Primary School, Plaintiffs Drennen, G.D., and Q.D.'s PII was input into PowerSchool's SIS.

602. Plaintiff Drennen received emails dated January 8, 2025, and January 10, 2025, notifying Plaintiff Drennen about the Data Breach.

603. As a result of the Data Breach and as recommended in the Notice, Plaintiff Drennen made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

604. After receiving the Notice, Plaintiff Drennen was notified by TransUnion that Plaintiff Q.D.'s Social Security Number was fraudulently utilized by a third party. As a result, Plaintiff Drennen spent several hours creating credit files for Plaintiffs Q.D. and G.D. and placing holds on those credit files.

605. Plaintiff Drennen has also spent significant time, including several hours of phone calls, responding to the Data Breach, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Drennen suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and

has increased concerns regarding the loss of her family's privacy, the fraudulent use of Plaintiff Q.D.'s Social Security Number, and potential further damages over the impact of cybercriminals accessing and using her family's PII.

606. PowerSchool was legally obligated to protect Plaintiffs Drennen, G.D., and Q.D.'s PII. Plaintiff Drennen would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

607. As a result of the Data Breach, Plaintiffs Drennen, G.D., and Q.D. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Drennen, G.D., and Q.D. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

qq. SOUTH CAROLINA PARENT SHAWN FRIEDMAN AND MINOR STUDENT J.F.

608. Plaintiff Shawn Friedman ("Plaintiff Friedman") and his minor child J.F. ("Plaintiff J.F.") are citizens and residents of South Carolina. At all relevant times, Plaintiff J.F. was a student at South Carolina Public Charter School District, which used PowerSchool's SIS. Plaintiff J.F. has been enrolled in the South Carolina Public Charter School District since August 2020. As a condition of Plaintiff J.F.'s enrollment, Plaintiffs Friedman and J.F.'s PII was input into PowerSchool's SIS, including but not limited to Plaintiff J.F.'s date of birth and social security number, Plaintiffs Friedman and J.F.'s home address, and Plaintiff Friedman's phone number.

609. Plaintiff J.F. received an email dated January 31, 2025, notifying Plaintiff J.F. of the Data Breach.

610. As a result of the Data Breach and as recommended in the Notice, Plaintiff Friedman made reasonable efforts to mitigate the impact of the Data Breach, including,

but not limited to, researching the Data Breach and seeking to protect his and his minor child's PII.

611. Plaintiff Friedman has spent significant time responding to the Data Breach on his own behalf and on behalf of Plaintiff J.F., including several hours of phone calls to banks and credit agencies, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Friedman was notified by Experian that Plaintiff J.F.'s information is available on the dark web, and has experienced issues with his credit. Plaintiff Friedman suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach, and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiff J.F.'s PII.

612. PowerSchool was legally obligated to protect Plaintiffs Friedman and J.F.'s PII. Plaintiff Friedman would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

613. As a result of the Data Breach, Plaintiffs Friedman and J.F. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Friedman and J.F. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

rr. SOUTH CAROLINA PARENT SAMARIAH LOCKHART AND MINOR STUDENT P.M.

614. Plaintiff Samariah Lockhart ("Plaintiff Lockhart") and her minor child P.M. ("Plaintiff P.M.") are citizens and residents of South Carolina. At all relevant times, Plaintiff P.M. was a student at Cyber Academy of South Carolina, which used PowerSchool's SIS. Plaintiff P.M. has been enrolled in the Cyber Academy of South

Carolina since October 2024. As a condition of Plaintiff P.M.'s enrollment, Plaintiff Lockhart's PII and Plaintiff P.M.'s PII and PHI were input into PowerSchool's SIS, including, but not limited to, Plaintiff P.M.'s date of birth, social security number, medical records, custody paperwork, Plaintiffs Lockhart and P.M.'s home address, Plaintiff Lockhart's email address and phone number, and additional information entered by Cyber Academy of South Carolina.

615. Plaintiff P.M. received an email dated January 10, 2025, notifying Plaintiff P.M. of the Data Breach.

616. As a result of the Data Breach and as recommended in the Notice, Plaintiff Lockhart made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and Plaintiff P.M.'s PII and PHI.

617. Plaintiff Lockhart has spent significant time responding to the Data Breach on behalf of herself and Plaintiff P.M., including dealing with increased spam and phishing emails and texts messages, spending time reviewing and securing financial accounts, addressing the hacking of Plaintiff P.M.'s bank account and Cash App accounts and subsequent unauthorized transactions shortly after the Data Breach, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Lockhart suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her own and Plaintiff P.M.'s privacy and potential further damages over the impact of cybercriminals accessing and using her own PII and Plaintiff P.M.'s PII and PHI.

618. PowerSchool was legally obligated to protect Plaintiffs Lockhart and P.M.'s PII and PHI. Plaintiff Lockhart would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if s/he had known PowerSchool

would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

619. Thus, as a result of the Data Breach, Plaintiffs Lockhart and P.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Lockhart and P.M. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

ss. SOUTH CAROLINA PARENT KRYSTAL VARGHA AND MINOR STUDENTS A.V. B.V. AND G.V.

620. Plaintiffs Krystal Vargha ("Plaintiff Vargha") and her minor children B.V. ("Plaintiff B.V."), A.V., ("Plaintiff A.V."), and G.V., ("Plaintiff G.V.") are citizens and residents of South Carolina. At all relevant times, Plaintiffs B.V., A.V., and G.V. were students in the Charleston County School District ("CCSD"), which used PowerSchool's SIS. Plaintiff B.V. was enrolled in Belle Hall Elementary School within the CCSD from August 2016 to May 2022 and in Laing Middle School within the CCSD from August 2022 to May 2025; Plaintiff A.V. was enrolled in Belle Hall Elementary School from August 2017 to May 2023 and in Laing Middle School from August 2023 to the present; and Plaintiff G.V. has been enrolled in Belle Hall Elementary School since August 2019. As a condition of Plaintiffs B.V., A.V., and G.V.'s enrollment, Plaintiff Vargha's PII and Plaintiffs B.V., A.V., and G.V.'s PII and PHI were input into PowerSchool's SIS, including but not limited to Plaintiffs B.V., A.V., and G.V.'s social security numbers and medical information, the family's address, and Plaintiff Vargha's email address.

621. Plaintiff Vargha received an email dated January 22, 2025, notifying her of the Data Breach.

622. As a result of the Data Breach and as recommended in the Notice, Plaintiff Vargha made reasonable efforts to mitigate the impact of the Data Breach, including,

but not limited to, researching the Data Breach, maintaining diligent review of her family's banking and other accounts, and seeking to protect her own and her minor children's PII and PHI.

623. Plaintiff Vargha has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs B.V., A.V., and G.V., including several hours of phone calls and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Vargha has experienced a string of attempts to access her email account, suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs B.V., A.V., and G.V.'s PII and PHI.

624. PowerSchool was legally obligated to protect Plaintiffs Vargha, B.V., A.V., and G.V.'s PII. Plaintiff Vargha would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

625. Thus, as a result of the Data Breach, Plaintiffs Vargha, B.V., A.V., and G.V. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Vargha, B.V., A.V., and G.V. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected, and safeguarded from future data breaches.

tt. TENNESSEE PARENT AMY LANCASTER AND MINOR STUDENTS E.M.L., K.C.L., AND C.S.R.L.

626. Plaintiffs Amy Lancaster ("Plaintiff Lancaster") and her minor children E.M.L., K.C.L., and C.S.R.L. ("Plaintiff E.M.L., K.C.L., and C.S.R.L.") are citizens and residents of Tennessee. At all relevant times, Plaintiffs E.M.L., K.C.L., and

C.S.R.L. were students in the Bartlett City School District, which used PowerSchool's SIS. Plaintiffs E.M.L., K.C.L., and C.S.R.L. have been enrolled in the Bartlett City School District since August 2021. As a condition of Plaintiffs E.M.L., K.C.L., and C.S.R.L.'s enrollment, Plaintiffs Lancaster, E.M.L., K.C.L., and C.S.R.L.'s PII and PHI were input into PowerSchool's SIS, including but not limited to immunization records, addresses, birth certificates, her marriage license, and Social Security Numbers.

627. Plaintiff Lancaster received an email dated January 13, 2025, notifying her about the Data Breach.

628. As a result of the Data Breach and as recommended in the Notice, Plaintiff Lancaster made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

629. Plaintiff Lancaster has spent time responding to the Data Breach on behalf of herself and Plaintiffs E.M.L., K.C.L., and C.S.R.L., including addressing an increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Lancaster suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs E.M.L., K.C.L., and C.S.R.L.'s PII and PHI.

630. PowerSchool was legally obligated to protect Plaintiffs Lancaster and E.M.L., K.C.L., and C.S.R.L.'s PII and PHI. Plaintiff Lancaster would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if Plaintiff Lancaster had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

631. Thus, as a result of the Data Breach, Plaintiffs Lancaster, E.M.L., K.C.L., and C.S.R.L. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Lancaster, E.M.L., K.C.L., and C.S.R.L. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

uu. TEXAS PARENT BETHANN JACKSON AND MINOR STUDENTS C.J. AND M.J.

632. Plaintiff Bethann Jackson ("Plaintiff Jackson") and her minor children C.J. ("Plaintiff C.J.") and M.J. ("Plaintiff M.J.") are citizens and residents of San Antonio, Texas. At all relevant times, Plaintiffs C.J. and M.J. were students at Great Heart Invictus School, which used PowerSchool's SIS. Plaintiffs C.J. and M.J. were enrolled in Great Heart Invictus School from January 2024 until the present. As a condition of Plaintiffs C.J. and M.J.'s enrollment, Plaintiff Jackson's PII and Plaintiffs C.J. and M.J.'s PII and PHI was input into PowerSchool's SIS.

633. Plaintiff Jackson received an email dated February 14, 2025, notifying Plaintiff Jackson of the Data Breach.

634. As a result of the Data Breach and as recommended in the Notice, Plaintiff Jackson made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, maintaining diligent review of her family's banking and other accounts, and seeking to protect her own and her minor children's PII and PHI.

635. Plaintiff Jackson has spent significant time responding to the Data Breach, including hours of phone calls, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Jackson has been notified by Experian that someone in California is using one of her children's social security number and that her child's

information is on the dark web. Plaintiff Jackson suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs C.J. and M.J.'s PII and PHI.

636. PowerSchool was legally obligated to protect Plaintiffs Jackson, C.J., and M.J.'s PII and PHI. Plaintiff Jackson would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

637. As a result of the Data Breach, Plaintiff Jackson, C.J., and M.J. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiff Jackson, C.J., and M.J. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

vv. TEXAS PARENT ASIA PRITCHETT AND MINOR STUDENT B.M.

638. Plaintiff Asia Pritchett ("Plaintiff Pritchett") and her minor child B.M. ("Plaintiff B.M.") are citizens and residents of Fort Worth, Texas. At all relevant times, Plaintiff B.M. was a student at Sue Crouch Intermediate School, which used PowerSchool's SIS. Plaintiff B.M. was enrolled in Sue Crouch Intermediate School from September 2024 until May 2025. As a condition of Plaintiff B.M.'s enrollment, Plaintiffs Pritchett and B.M.'s PII was input into PowerSchool's SIS.

639. Plaintiff Pritchett received an email dated February 25, 2025, and an email dated March 2, 2025, notifying her of the Data Breach.

640. As a result of the Data Breach and as recommended in the Notice, Plaintiff Pritchett made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, maintaining diligent review of her

family's banking and other accounts, and seeking to protect her own and her minor child's PII.

641. Plaintiff Pritchett has spent significant time responding to the Data Breach on her own behalf and on behalf of Plaintiff B.M., including hours of phone calls, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. In December 2024, Plaintiff Pritchett was notified by her bank that her account was compromised. Someone also hacked into her Wise account and withdrew the funds. Additionally, her credit report contains inaccuracies and credit card inquiries that she did not make. Plaintiff Pritchett suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiff B.M.'s PII.

642. PowerSchool was legally obligated to protect Plaintiffs Parent Pritchett and Child B.M.'s PII. Plaintiff Pritchett would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

643. As a result of the Data Breach, Plaintiff Pritchett and her minor child have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiff Pritchett and her child have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

ww. UTAH PARENT JOSEPH HAUPTMAN AND MINOR STUDENTS D.H. AND M.H.

644. Plaintiff Joseph Hauptman ("Plaintiff Hauptman") and his minor children D.H. ("Plaintiff D.H.") and M.H. (Plaintiff M.H.) are citizens and residents of Utah. At all relevant times, Plaintiffs D.H. and M.H. were students at Cache County School

District, which used PowerSchool's SIS. Plaintiff D.H. has been enrolled in the Cache County School District since August 2016 and Plaintiff M.H. has been enrolled in the Cache County School District since October 2014. As a condition of Plaintiffs D.H. and M.H.'s enrollment as students at Cache County School District, Plaintiffs Hauptman, D.H., and M.H.'s PII were input into PowerSchool's SIS.

645. Plaintiff Hauptman received emails dated January 7, 2025, and January 9, 2025, notifying "parents and guardians" of the Data Breach.

646. As a result of the Data Breach and as recommended in the Notice, Plaintiff Hauptman made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his own and his minor children's PII.

647. Plaintiff Hauptman has spent significant time, including spending time on emails, reviewing and securing financial accounts, changing passwords, and otherwise responding to the Data Breach on behalf of himself and Plaintiffs D.H. and M.H. and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Hauptman has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiffs D.H. and M.H.'s PII.

648. PowerSchool was legally obligated to protect Plaintiffs Hauptman, D.H., and M.H.'s PII. Plaintiff Hauptman would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

649. As a result of the Data Breach, Plaintiffs Hauptman, D.H., and M.H. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Hauptman, D.H., and M.H. have a continuing interest in

ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

xx. VIRGINIA PARENT ELEANOR TILLMAN AND MINOR STUDENT L.L.

650. Plaintiffs Eleanor Louise Tillman ("Plaintiff Tillman") and her minor child L.L. ("Plaintiff L.L.") are citizens and residents of Virginia. At all relevant times, Plaintiff L.L. was a student at Botetourt County Public Schools, which used PowerSchool's SIS. Plaintiff L.L. has been enrolled at Botetourt County Public Schools since August 2024. As a condition of Plaintiff L.L.'s enrollment, Plaintiffs Tillman and L.L.'s PII were input into PowerSchool's SIS, including but not limited to birth certificates and Social Security Numbers.

651. Plaintiff Tillman received an email dated January 10, 2025, notifying Tillman about the Data Breach.

652. As a result of the Data Breach and as recommended in the Notice, Plaintiff Tillman made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor child's PII.

653. Plaintiff Tillman has spent significant time responding to the Data Breach on behalf of herself and Plaintiff L.L., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Tillman experienced unauthorized charges for fraudulent purchases on her account which required additional time spent with the bank and debit card cancellation. Plaintiff Tillman suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the

loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and L.L.'s PII.

654. PowerSchool was legally obligated to protect Plaintiffs Tillman and L.L.'s PII. Plaintiff Tillman would not have allowed Plaintiffs Tillman and L.L.'s PII to be shared with or accessible by PowerSchool if Plaintiff Tillman had known PowerSchool would not maintain sufficient data security safeguards to adequately protect Plaintiffs Tillman and L.L.'s PII.

655. Thus, as a result of the Data Breach, Plaintiffs Tillman and L.L. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for Plaintiffs Tillman and L.L.'s lifetimes. Plaintiffs Tillman and L.L. have a continuing interest in ensuring that Plaintiffs Tillman and L.L.'s PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

yy. VIRGINIA PARENT TOWFEQ ZARIF AND MINOR STUDENT P.Z.

656. Plaintiff Towfeq Zarif ("Plaintiff Zarif") and his minor child P. Z. ("Plaintiff P.Z.") are citizens and residents of Virginia. At all relevant times, Plaintiff P. Z. was a student of Baldwin Elementary, which used PowerSchool's SIS. Plaintiff has been enrolled at Baldwin Elementary since December 2023. As a condition of Plaintiff P. Z.'s enrollment, Plaintiffs Zarif and P. Z.'s PII was input into PowerSchool's SIS to promote interoperability of educational services.

657. Plaintiff Zarif received an email from Baldwin Elementary on January 10, 2025, notifying him of the Data Breach.

658. As a result of the Data Breach and as recommended in the Notice, Plaintiff Zarif made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect his minor child's PII.

659. Plaintiff Zarif has spent significant time responding to the Data Breach on behalf of himself and Plaintiff P. Z., including addressing a noticeable increase in spam communications, and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Zarif suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his family's privacy and potential further damages over the impact of cybercriminals accessing and using his own and Plaintiff P. Z.'s PII.

660. PowerSchool was legally obligated to protect Plaintiffs Zarif and P.Z.'s PII. Plaintiff Zarif would not have allowed his family's PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

661. As a result of the Data Breach, Plaintiffs Zarif and P. Z. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Zarif and P. Z. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

zz. WASHINGTON PARENT EMILY PEASE AND MINOR STUDENTS A.E.J.A., A.R.R., AND A.E.R.

662. Plaintiffs Emily Pease ("Plaintiff Pease") and her minor children, A.E.J.A. ("Plaintiff A.E.J.A."), A.R.R. ("Plaintiff A.R.R.") and A.E.R. (Plaintiff A.E.R.") are citizens and residents of Washington. At all relevant times, Plaintiffs A.E.J.A., A.R.R., and A.E.R. were students at Barbara McClintock STEM Elementary, which used PowerSchool's SIS. Plaintiffs A.E.J.A., A.R.R., and A.E.R. have been enrolled at Barbara McClintock STEM Elementary since August of 2021, 2022, and 2024 respectively. As a condition of Plaintiffs A.E.J.A., A.R.R., and A.E.R.'s enrollment, Plaintiffs Pease, A.E.J.A., A.R.R., and A.E.R.'s PII and PHI were input into

PowerSchool's SIS, including but not limited to birth dates, addresses, social security numbers, immunization records, and additional information input by the school.

663. Plaintiff Pease received an email in January 2025, notifying her of the Data Breach.

664. As a result of the Data Breach and as recommended in the Notice, Plaintiff Pease made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

665. Plaintiff Pease has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs A.E.J.A., A.R.R., and A.E.R., including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Since the Data Breach, Plaintiff Pease has received an increased number of fraudulent spam calls regarding her bank accounts. Plaintiff Pease suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs A.E.J.A., A.R.R., and A.E.R.'s PII and PHI.

666. PowerSchool was legally obligated to protect Plaintiffs Pease, A.E.J.A., A.R.R., and A.E.R.'s PII and PHI. Plaintiff Pease would not have allowed her family's PII and PHI to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

667. Thus, as a result of the Data Breach, Plaintiffs Pease and A.E.J.A., A.R.R., and A.E.R. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Pease, A.E.J.A., A.R.R., and A.E.R. have

a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

aaa. WASHINGTON PARENT HEATHER TAYLOR AND MINOR STUDENTS B.N.T. AND B.A.T.

668. Plaintiff Heather Taylor ("Plaintiff Taylor") and her minor children B.N.T. (Plaintiff B.N.T.) and B.A.T. (Plaintiff B.A.T.) are citizens and residents of Washington. At all relevant times, Plaintiffs B.N.T. and B.A.T. were students at Mountainside Middle School, which used PowerSchool's SIS at all relevant times. Plaintiffs B.N.T. and B.A.T. were enrolled in Mountainside Middle School from August, 2022 until present. As a condition of Plaintiffs B.N.T. and B.A.T.'s enrollment, Plaintiffs Taylor, B.N.T. and B.A.T.'s PII were input into PowerSchool's SIS to promote interoperability of educational services, including but not limited to Plaintiffs Taylor, B.N.T., and B.A.T.'s birth dates, phone number, address, and other information about Plaintiffs B.N.T. and B.A.T. in the possession of Mountainside Middle School.

669. Plaintiff Taylor received emails dated January 10, 2025, January 16, 2025, January 23, 2025, March 2, 2025, and March 3, 2025, notifying her of the Data Breach.

670. As a result of the Data Breach and as recommended in the Notices, Plaintiff Taylor made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, maintaining diligent review of her banking and other accounts, and seeking to protect her own and her minor children's PII.

671. Plaintiff Taylor has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs B.N.T. and B.A.T, including several hours of phone calls and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Taylor suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of

the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs B.N.T. and B.A.T.'s PII.

672. PowerSchool was legally obligated to protect Plaintiffs Taylor, B.N.T., and B.A.T.'s PII. Plaintiff Taylor would not have allowed her family's PII to be shared with or accessible by PowerSchool if s/he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

673. Thus, as a result of the Data Breach, Plaintiffs Taylor, B.N.T., and B.A.T. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetime. Plaintiffs Taylor, B.N.T., and B.A.T. have a continuing interest in ensuring that their PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

bbb. WISCONSIN PARENT MICHELLE LA COUNT AND MINOR STUDENTS E.R.M. AND R.E.M.

674. Plaintiff Michelle La Count ("Plaintiff La Count") and her minor children E.R.M. ("Plaintiff E.R.M.") and R.E.M. (Plaintiff R.E.M.") are citizens and residents of Wisconsin. At all relevant times, Plaintiffs E.R.M. and R.E.M. were students at Lineville Intermediate and Meadowbrook Elementary, respectively, in the Howard-Suamico School District, which used PowerSchool's SIS. Plaintiffs E.R.M. and R.E.M have been enrolled since the 2020 school year, both attending Meadowbrook Elementary, with Plaintiff E.R.M moving to Lineville Intermediate in 2023. As a condition of Plaintiffs E.R.M. and R.E.M.'s enrollment, Plaintiff La Count's PII and Plaintiffs E.R.M. and R.E.M.'s PII and PHI were input into PowerSchool's SIS to promote interoperability of educational services, including but not limited to Plaintiffs E.R.M. and R.E.M.'s enrollment, medical, and contact information, and Plaintiff La Count's phone number and email address.

675. Via an email sent to Plaintiff La Count dated January 8, 2025, Plaintiffs E.R.M. and R.E.M were notified of the Data Breach.

676. As a result of the Data Breach and as recommended in the Notice, Plaintiff La Count made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and her minor children's PII and PHI.

677. Plaintiff La Count has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs E.R.M. and R.E.M., including addressing an increase in spam texts and calls, and several hours reviewing credit reports and financial records, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff La Count suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs E.R.M. and R.E.M.'s PII and PHI.

678. PowerSchool was legally obligated to protect Plaintiffs La Count, E.R.M., and R.E.M.'s PII and PHI. Plaintiff La Count would not have allowed her family's PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII and PHI.

679. Thus, as a result of the Data Breach, Plaintiffs La Count, E.R.M., and R.E.M. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs La Count, E.R.M., and R.E.M. have a continuing interest in ensuring that their PII and PHI, which upon information and belief remain in PowerSchool's possession, are protected and safeguarded from future data breaches.

ccc. WYOMING PARENT SKYE BREANN LAWSON AND MINOR STUDENTS B.L. AND H.L.

680. Plaintiff Skye Breann Lawson ("Plaintiff Lawson") and her minor children B.L. ("Plaintiff B.L."), and H.L. ("Plaintiff H.L."), are citizens and residents of Wyoming. At all relevant times, Plaintiff B.L. was a student at Evanston Middle School and Plaintiff H.L. was a student at North Evanston Elementary School, both of which used PowerSchool's SIS. Plaintiff B.L. has been enrolled at Evanston Middle School since August 2024, and before that was a student at North Evanston Elementary School. Plaintiff H.L. has been enrolled at North Evanston Elementary School since August 2022. As a condition of Plaintiffs B.L. and H.L.'s enrollment, Plaintiffs Lawson, B.L., and H.L.'s PII were input into PowerSchool's SIS, including but not limited to addresses, phone numbers, names, social security numbers, and additional data input by the schools.

681. Plaintiff Lawson received an email dated March 7, 2025, notifying her of the Data Breach.

682. As a result of the Data Breach and as recommended in the Notice, Plaintiff Lawson made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and seeking to protect her own and Plaintiffs B.L. and H.L.'s PII.

683. Plaintiff Lawson has spent significant time responding to the Data Breach on behalf of herself and Plaintiffs B.L. and H.L., including addressing a noticeable increase in spam calls, text messages, and emails that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, childcare, and/or recreation. Plaintiff Lawson suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the

loss of her family's privacy and potential further damages over the impact of cybercriminals accessing and using her own and Plaintiffs B.L. and H.L.'s PII.

684. PowerSchool was legally obligated to protect Plaintiffs Lawson, B.L. and H.L.'s PII. Plaintiff Lawson would not have allowed her family's PII to be shared with or accessible by PowerSchool if Plaintiff Lawson had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

685. As a result of the Data Breach, Plaintiffs Lawson, B.L. and H.L. have faced, and will continue to face, a present and continuing risk of fraud and identity theft for their lifetimes. Plaintiffs Lawson, B.L. and H.L. have a continuing interest in ensuring that their PII, which upon information and belief remain in PowerSchool's possession, is protected and safeguarded from future data breaches.

4. FORMER STUDENTS

a. COLORADO FORMER STUDENT KENNAH J. WHITE

686. Plaintiff Kennah J. White is a citizen of Colorado and resides in Colorado Springs, Colorado. At all relevant times, Plaintiff Kennah J. White was a student of Colorado Springs School District 11, which used PowerSchool's SIS. Plaintiff White was enrolled in Holmes Middle School and Coronado High School operated by the Colorado Springs School District 11 from August 2020 until May 2025. As a condition of Plaintiff White's enrollment as a student, Plaintiff White's PII and PHI were input into PowerSchool's SIS.

687. Plaintiff White received an email dated January 13, 2025, notifying Plaintiff White about the Data Breach.

688. As a result of the Data Breach and as recommended in the Notice, Plaintiff White made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

689. Plaintiff White has spent significant time responding to the Data Breach, including addressing a noticeable increase in spam calls and messages and several hours of phone calls, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation. Plaintiff White suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII and PHI.

690. PowerSchool was legally obligated to protect Plaintiff White's PII and PHI. Plaintiff White would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

691. As a result of the Data Breach, Plaintiff White has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff White has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

b. IOWA FORMER STUDENT ALEXANDER LARSON

692. Plaintiff Alexander Larson ("Plaintiff Larson") is a citizen and current resident of Eau Claire, Wisconsin. At all relevant times, Plaintiff Larson was a student at Iowa Falls-Alden High School, which used PowerSchool's SIS. Plaintiff Larson was enrolled in Iowa Falls-Alden High School from August 2020 until May 2024. As a condition of Plaintiff Larson's enrollment and receipt of educational services, Plaintiff Larson's PII and PHI were input into PowerSchool's SIS.

693. Plaintiff Larson received an email dated February 25, 2025, notifying him of the Data Breach.

694. As a result of the Data Breach and as recommended in the Notice, Plaintiff Larson made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

695. Plaintiff Larson has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Larson suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI.

696. PowerSchool was legally obligated to protect Plaintiff Larson's PII and PHI.

697. As a result of the Data Breach, Plaintiff Larson has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Larson has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

c. KANSAS FORMER STUDENT LAUREN OVERLY

698. Plaintiff Lauren Overly ("Plaintiff Overly") is a citizen and current resident of Kansas. At all relevant times, Plaintiff Overly was a student at El Dorado Public School, Kansas, which used PowerSchool's SIS. Plaintiff Overly was enrolled at El Dorado Public School from August 2002 until May 2015. As a condition of Plaintiff Overly's enrollment, Plaintiff Overly's PII and PHI were input into PowerSchool's SIS.

699. As a result of the Data Breach, Plaintiff Overly made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

700. Plaintiff Overly has spent significant time responding to the Data Breach, including researching the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Overly suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII and PHI.

701. PowerSchool was legally obligated to protect Plaintiff Overly's PII and PHI.

702. Thus, as a result of the Data Breach, Plaintiff Overly has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Overly has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

d. KANSAS FORMER STUDENT EMMA PANGRACS

703. Plaintiff Emma Pangracs ("Plaintiff Pangracs") is a citizen and current resident of Missouri. At all relevant times, Plaintiff Pangracs was a student at El Dorado Public School, Kansas, which used PowerSchool's SIS. Plaintiff Pangracs was enrolled at El Dorado Public School from August 2005 until May 2010. As a condition of Plaintiff Pangracs's enrollment, Plaintiff Pangracs's PII and PHI were input into PowerSchool's SIS, including but not limited to her date of birth, social security number, and vaccination information.

704. As a result of the Data Breach, Plaintiff Pangracs made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

705. Plaintiff Pangracs has spent significant time responding to the Data Breach, including researching the Data Breach and maintaining diligent review of her banking and other accounts and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Pangracs suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII and PHI.

706. PowerSchool was legally obligated to protect Plaintiff Pangracs's PII and PHI.

707. Thus, as a result of the Data Breach, Plaintiff Pangracs has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Pangracs has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

e. MAINE FORMER STUDENT ZANDER NORCIA

708. Plaintiff Zander Norcia ("Plaintiff Norcia") is a citizen and resident of Maine. At all relevant times, Plaintiff Norcia was a student at Baxter Academy, which used PowerSchool's SIS. Plaintiff Norcia was enrolled in Baxter Academy from August 2021 until May 2025. As a condition of Plaintiff Norcia's enrollment, Plaintiff Norcia's PII and PHI were input into PowerSchool's SIS.

709. Plaintiff Norcia received an email dated February 27, 2025, notifying him of the Data Breach.

710. As a result of the Data Breach and as recommended in the Notice, Plaintiff Norcia made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

711. Plaintiff Norcia has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Since the Data Breach a few of Plaintiff's accounts were logged into without his permission. Plaintiff Norcia suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI.

712. PowerSchool was legally obligated to protect Plaintiff Norcia's PII and PHI. Had he the choice, Plaintiff Norcia would not have allowed his PII and PHI to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect his PII and PHI.

713. Thus, as a result of the Data Breach, Plaintiff Norcia has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Norcia has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

f. MISSOURI FORMER STUDENT JACOB ISLAS

714. Plaintiff Jacob Islas ("Plaintiff Islas") is a citizen and current resident of Missouri. At all relevant times, Plaintiff Islas was a student at Liberty Public Schools in Liberty, Missouri, which used PowerSchool's SIS. Plaintiff Islas was enrolled at Liberty Public Schools from August 2007 until May 2020. As a condition of Plaintiff Islas' enrollment, Plaintiff Islas' PII and PHI were input into PowerSchool's SIS.

715. As a result of the Data Breach, Plaintiff Islas made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

716. Plaintiff Islas has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Islas suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI.

717. PowerSchool was legally obligated to protect Plaintiff Islas' PII and PHI.

718. Thus, as a result of the Data Breach, Plaintiff Islas has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Islas has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

g. NORTH CAROLINA FORMER STUDENT AYEDON BAUDER

719. Plaintiff Ayedon Bauder ("Plaintiff Bauder") is a citizen and resident of North Carolina. At all relevant times, Plaintiff Bauder was a student at Winston-Salem/Forsyth County School District, which used PowerSchool's SIS. Plaintiff Bauder was enrolled in the Winston-Salem/Forsyth County School District from August 2021 until June 2025. As a condition of Plaintiff Bauder's enrollment as a student at Winston-Salem/Forsyth County School District, Plaintiff Bauder's PII was input into PowerSchool's SIS.

720. Plaintiff Bauder's parents received an email dated January 8, 2025, notifying them of the Data Breach.

721. As a result of the Data Breach and as recommended in the Notice, Plaintiff Bauder made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

722. Plaintiff Bauder has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Bauder suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII.

723. PowerSchool was legally obligated to protect Plaintiff Bauder's PII. Had he the choice, Plaintiff Bauder would not have allowed his PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect his PII.

724. Thus, as a result of the Data Breach, Plaintiff Bauder has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Bauder has a continuing interest in ensuring that his PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

h. OHIO FORMER STUDENT EVAN GRAMELSPACHER

725. Plaintiff Evan Gramelspacher ("Plaintiff Gramelspacher") is a citizen and resident of Ohio. At all relevant times, Plaintiff Gramelspacher was a student of the Olentangy Local School District, which used PowerSchool's SIS. Plaintiff Gramelspacher was enrolled in the Olentangy Local School District from August 2012 until May 2025. As a condition of Plaintiff Gramelspacher's enrollment as a student of

the Olentangy Local School District, Plaintiff Gramelspacher's PII and PHI was input into PowerSchool's SIS.

726. Plaintiff Gramelspacher's parent received an email dated January 30, 2025, notifying Plaintiff Gramelspacher of the Data Breach.

727. As a result of the Data Breach and as recommended in the Notice, Plaintiff Gramelspacher made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

728. Plaintiff Gramelspacher has spent significant time, including several hours of phone calls responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Gramelspacher suffers lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI.

729. PowerSchool was legally obligated to protect Plaintiff Gramelspacher's PII and PHI. Had he the choice, Plaintiff Gramelspacher would not have allowed his PII to be shared with or accessible by PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

730. Thus, as a result of the Data Breach, Plaintiff Gramelspacher has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Gramelspacher has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

i. TEXAS FORMER STUDENT STEFAN SPANN

731. Plaintiff Stefan Spann ("Plaintiff Spann") is a citizen and resident of Lorena, Texas. At all relevant times, Plaintiff Spann was a student at Lorena

Independent School District, which used PowerSchool's SIS. Plaintiff Spann was enrolled in Lorena Independent School District from August 2010 until May 2021. As a condition of Plaintiff Spann's enrollment, Plaintiff Spann's PII and PHI was input into PowerSchool's SIS.

732. Plaintiff Spann received an email dated February 15, 2025, notifying him of the Data Breach.

733. As a result of the Data Breach and as recommended in the Notice, Plaintiff Spann made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of his banking and other accounts.

734. Plaintiff Spann has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Spann suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI.

735. PowerSchool was legally obligated to protect Plaintiff Spann's PII and PHI. Had he the choice, Plaintiff Spann would not allowed his PII and PHI to be shared with or accessible to PowerSchool if he had known PowerSchool would not maintain sufficient data security safeguards to adequately protect his PII and PHI.

736. Thus, as a result of the Data Breach, Plaintiff Spann has faced, and will continue to face, a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Spann have a continuing interest in ensuring that his PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

j. UTAH FORMER STUDENT HAILEY MCCALL SHINGLETON

737. Plaintiff Hailey McCall Shingleton ("Plaintiff Shingleton") is a citizen and current resident of Salt Lake City, Utah. At all relevant times, Plaintiff Shingleton was a student at Hillside Middle and Highland High School, part of the Salt Lake City School District, which used PowerSchool's SIS. Plaintiff Shingleton was enrolled in Hillside Middle School and Highland High School from 2008-2015. As a condition of Plaintiff Shingleton's enrollment, Plaintiff Shingleton's PII was input into PowerSchool's SIS.

738. Plaintiff Shingleton received an email forwarded to her dated March 09, 2025, notifying her of the Data Breach.

739. As a result of the Data Breach and as recommended in the Notice, Plaintiff Shingleton made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her banking and other accounts.

740. Plaintiff Shingleton has spent significant time responding to the Data Breach, including addressing a noticeable increase in spam calls, emails and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Shingleton suffered lost time, annoyance, interference, emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII.

741. PowerSchool was legally obligated to protect Plaintiff Shingleton's PII. Plaintiff Shingleton would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect her PII.

742. Thus, as a result of the Data Breach, Plaintiff Shingleton has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Shingleton has a continuing interest in ensuring that her PII, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

k. WISCONSIN FORMER STUDENT KAYELEEN CAMPBELL

743. Plaintiff Kayeleen Campbell ("Plaintiff Campbell") is a citizen and resident of Illinois. At all relevant times, Plaintiff Campbell was a student of the St. Croix Falls School District, located in St. Croix Falls, Wisconsin, which used PowerSchool's SIS. Plaintiff Campbell was enrolled in the St. Croix Falls School District from elementary school until her graduation from St. Croix Falls High School in 2017. As a condition of Plaintiff Campbell's enrollment as a student, Plaintiff Campbell's PII and PHI were input into PowerSchool's SIS.

744. Plaintiff Campbell received notice of the Data Breach from a Facebook post on the St. Croix Falls School District's Facebook page and a follow-up phone call with the St. Croix Falls School District.

745. As a result of the Data Breach and as recommended in the notice and follow-up with the St. Croix Falls School District, Plaintiff Campbell made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and maintaining diligent review of her tax, banking and other accounts.

746. Plaintiff Campbell has spent significant time, including, including addressing a noticeable increase in spam calls and messages that interfere with work duties and personal time, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work, taking care of her children, and recreation. Plaintiff Campbell suffered lost time, annoyance, interference,

emotional distress, and inconvenience as a result of the Data Breach and has increased concerns regarding the loss of her privacy and potential further damages over the impact of cybercriminals accessing and using her PII and PHI and using that information to access the PII and PHI of her minor children.

747. PowerSchool was legally obligated to protect Plaintiff Campbell's PII and PHI. Had she the choice, Plaintiff Campbell would not have allowed her PII to be shared with or accessible by PowerSchool if she had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

748. Thus, as a result of the Data Breach, Plaintiff Campbell has faced, and will continue to face, a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Campbell has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains in PowerSchool's possession, is protected and safeguarded from future data breaches.

5. TEACHER'S UNIONS

749. Plaintiff PTU is a professional organization consisting of over 2000 members, including regularly appointed teachers, long-term substitutes, and long-term substitutes in pool in Providence, Rhode Island. At all relevant times, PTU members used PowerSchool SIS as part of their employment. As a condition of their employment, at least some PTU members input their PII and/or PHI into PowerSchool's SIS.

750. As a result of the Data Breach, PTU has had to expend time and resources to assist members in mitigating the impact of the Breach, including by members have had to, and will have to, take measures that would not otherwise be necessary to protect against identity theft and/or credit disruptions. Moreover, PTU has had to expend resources to address members' concerns and experiences as a result of the breach, including answering member calls and questions regarding the breach, the impact of

the breach on their employment and potential need to continue using the PowerSchool software.

751. Thus, Plaintiff PTU has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

752. PowerSchool was legally obligated to protect Plaintiff PTU's members' PII and PHI. Had PTU members the choice, Plaintiff PTU's members would not have allowed their PII to be shared with or accessible to a software service like PowerSchool if they had known PowerSchool would not maintain sufficient data security safeguards to adequately protect their PII.

V. CLASS ALLEGATIONS

753. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

754. Plaintiffs seek to represent the following Classes or Subclasses defined as follows:[287]

755. **Nationwide Class**: All United States residents whose PII and/or PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all those who were sent notice of the Data Breach.

756. **Student Subclass**: All current or former students residing in the United States whose PII and/or PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all those who were sent notice of the Data Breach.

757. **Parent Subclass**: All parents of current or former students residing in the United States whose PII and/or PHI was accessed by and disclosed to unauthorized persons in the Data Breach including, all those who were sent notice of the data breach.

758. **Teacher Subclass**: All current or former employees of educational institutions residing in the United States whose PII and/or PHI was accessed by and

[287] Plaintiffs reserve the rights to alter, amend, or alternatively pursue the Class definitions.

disclosed to unauthorized persons in the Data Breach including, all those who were sent notice of the Data Breach.

759. **Teacher's Union Subclass**: All teacher's unions registered in the United States whose member(s) had their PII and/or PHI accessed by and disclosed to unauthorized persons in the Data Breach including, all those who were sent notice of the data breach. [288]

760. Excluded from the Class are the following individuals and/or entities: (i) any Judge or Magistrate presiding over this action, any members of their immediate families, and any of their staff; (ii) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, assigns, current and former employees, officers, and directors, and any entity in which the Defendants have a controlling interest; and (iii) Plaintiffs' counsel and Defendants' counsel.

761. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

762. Numerosity (Rule 23(a)(1)): The exact number of members of the Class is unknown and currently unavailable to Plaintiffs, but joinder of individual members herein is impractical. The Class is likely comprised of thousands of individuals. Defendants retain the data of fifty (50) million students, each of whom could be a member of the Class, and each of whom may have a guardian or multiple guardians who could also be a member of the Class. The precise number of Class Members, including their addresses, are unknown to Plaintiffs at this time, but can be ascertained from PowerSchool's records. The Class Members may be notified of the pendency of this action by mail or email, internet postings and/or publications, and supplemented (if deemed necessary or appropriate by the Court) by published notice.

763. Predominant Common Questions of Law and Fact (Rule 23(a)(2)): The Class's claims present common questions of law and fact, and those questions

[288] State Subclasses: Plaintiffs representative of each state define subclasses for each state as: All current or former employees, students, parents (of current or former students)

predominate over any questions that may affect individual Class members. The common and legal questions include, without limitation:

i. Whether Defendants had a duty to protect the PII of Plaintiffs and Class Members;

ii. Whether Defendants had a duty not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

iii. Whether Defendants failed to adequately secure and safeguard the PII of Plaintiffs and Class Members;

iv. Whether Defendants timely learned of the Data Breach;

v. Whether Defendants made an untimely disclosure of the Data Breach to Plaintiffs and Class Members;

vi. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate for the nature and scope of the information compromised in the Data Breach;

vii. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to secure and safeguard the PII of Plaintiffs and Class Members;

viii. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

ix. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

x. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of the Data Breach.

764. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of the claims of the Class because Plaintiffs, like all other Class Members, had their PII compromised in the Data Breach, suffered damages as a result of that Data Breach, and seek the same relief as the Class Members.

765. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs adequately represent the Class because their interests do not conflict with the interests of Class Members, and they have retained counsel competent and experienced in complex class

residing in and teacher's unions registered in their state of residency whose PII and/or PHI was accessed by and disclosed to unauthorized persons in the Data Breach including, all those who were sent notice of the Data Breach.

actions and consumer litigation. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class.

766. Superiority (Rule 23(b)(3)): A class action is superior to other available means of adjudication for this controversy. It would be impracticable for Class Members to individually litigate their own claims against Defendants because the damages suffered by Plaintiffs and the members of the Class are relatively small compared to the cost of individually litigating their claims. Individual litigation would create the potential for inconsistent judgments and delay and expenses to the court system. A class action provides an efficient means for adjudication with fewer management difficulties and comprehensive supervision by a single court.

COUNT I – NEGLIGENCE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

(AGAINST ALL DEFENDANTS)

767. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

768. Plaintiffs and Class Members were required to submit their non-public PII to PowerSchool in order to receive services from PowerSchool's educational entity clients.

769. In providing their PII, Plaintiffs and Class Members had a reasonable expectation that this information would be securely maintained and not easily accessible to, unreasonably accessible to or exfiltrated by others, including cybercriminals.

770. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard its computer system – and Plaintiffs' and Class Members' PII held within it – to prevent disclosure of the information, and to safeguard the information from unauthorized access and theft. PowerSchool's duty

included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious manner, mitigate its damage and to give prompt notice to those affected in the event of a data breach.

771. Defendants PowerSchool and Bain Capital owed a duty of care to take reasonable measures to ensure that the agents and associates they entrusted with Plaintiffs' and Class Members PII, including Movate, implemented adequate data security practices to prevent unauthorized third parties to access.

772. In addition to those duties, as a subcontractor of Defendants PowerSchool and Bain Capital, Defendant Movate had additional, independent, non-delegable duties that it owed to Plaintiffs and Class Members to hire competent employees and agents and to train and supervise them to ensure they recognize the duties owed to Plaintiffs and Class Members. In providing technical support services with access to millions of individuals' highly sensitive data, Movate also had a duty to take reasonable steps to ensure adequate data security procedures and practices sufficient to maintain confidentiality of the PII.

773. Defendants owed a common law duty to Plaintiffs and Class Members to prevent foreseeable harm. The risk that unauthorized persons would attempt to gain access to databases of PII and misuse it was foreseeable to Defendants, given that PowerSchool holds, and Movate was given access to, vast amounts of PII, including large subsets of data pertaining to vulnerable minors.

774. After all, PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class Members. Thus, Defendants knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

775. Defendants owed a duty of care to Plaintiffs and Class Members to provide and maintain data security consistent with industry standards and other requirements discussed herein, and to ensure that PowerSchool's and its service

provider systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members. This duty included, among other things, designing, maintaining, monitoring, and testing relevant security systems, protocols, and practices to ensure that Plaintiffs' and Class Members' information was adequately secured from unauthorized access. For PowerSchool, this duty also included, at the minimum, that Plaintiffs' and Class Members' PII be maintained in accordance with industry standards, including: 1) implementation of multifactor authentication (2) implementation of the principle of least privileges, (3) implementation of the principle of network segmentation, (4) implementation of rate limiting, (5) securing the contractor's credentials, (6) monitoring its logs for unusual activity, (7) adequately implementing an intrusion detection and prevention system, and (8) encrypting the Data; (9) appropriate requirements regarding regular password changes and (10) supervision over those with access to valuable PII. PowerSchool also had a duty to delete any PII that was no longer needed to serve client needs.

776. In addition to the above, Defendant Movate owed a duty to Plaintiffs and Class Members to exercise the requisite standard of care to monitor and audit the security protocol and practices of its employees and agents who had access to Plaintiffs' and Class Members' PII. Specifically, Defendant Movate owed a duty to, among other things: (1) appropriately train its employees to secure their credentials; (2) rotate its employees' credentials; (3) and implement the principle of least privileges for data systems' access.

777. PowerSchool's privacy policy, publicly made available on its website, acknowledged its duty to adequately protect Plaintiffs' and Class Members' PII. Specifically, PowerSchool represents that, "PowerSchool places great importance and value on the proper handling of personal data that flows within our product as we provide services to our customers." PowerSchool states the following with regard to security: "We seek to protect our customers' personal data from unauthorized access,

use, modification, disclosure, loss, or theft by leveraging various reasonable security methods to secure our customers' personal data throughout its processing lifecycle with PowerSchool applications."[288]

778. Also on that website is PowerSchool's Global Privacy Statement in place on October 1, 2024 and last updated on July 1, 2025,. That Statement indicates "[w]hether PowerSchool is a collector or processor or your data, PowerSchool is committed to protecting your personal information. PowerSchool uses commercially reasonable physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and availability of your personal information…" It also claims that "[a]s customers provide PowerSchool with Customer Data to process, PowerSchool makes commercially reasonable efforts to ensure the security of our systems." *Id.* Defendant PowerSchool has undertaken similar duties or privacy and data protection in each state it operates. *See*, https://www.powerschool.com/wp-content/uploads/PowerSchool-Service-Agreements/Customer_State_DPA_List_March_2024.pdf. *See also, Cybersecurity, Data Privacy, & Infrastructure, Powerschool*, https://www.powerschool.com/security (last visited Jan. 17, 2025), *supra*, at note 30. PowerSchool had a duty to avoid intentional and negligent misrepresentations, independent of any contractual obligation.

779. As a corporate entity that holds itself out as a trusted provider of educational support services and is in a superior position to protect against the harm suffered by Plaintiffs and Class Members, PowerSchool assumed a duty to reasonably safeguard their PII.

780. Defendant Movate's Associate Vice President and Head of Information Security likewise represented that it is certified as compliant under the ISO 27001:2013

[288] PowerSchool website at "PowerSchool: Global Privacy Statement." last updated July 1, 2025, available at PowerSchool's website (last accessed August 04, 2025): https://www.powerschool.com/privacy/

framework across North America, Asia (including offices in the Philippines), Africa, Latin America, and Europe. Thus, Movate held itself out as having undertaken certain security measures and safeguards.

781. Defendants' duty of care to use reasonable security measures to protect the PII in their possession also arose because of the special relationship that existed between Defendants and Plaintiffs and Class Members, including the vulnerable population of minors, which is recognized by federal and state statutes and regulations, as well as by common law. Defendants were each in a superior position to ensure that its own, and its service providers' systems, were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach. By accepting, taking possession, collecting, storing, processing, and accessing Plaintiffs' and Class Members' highly sensitive data, PowerSchool formed a special relationship and became a guardian of Plaintiffs' and Class Members' PII.

782. Defendants are morally culpable, given the prominence of security breaches in educational institutional settings, and because it knew of numerous, other well-publicized data breaches.

783. Defendants owed a duty to implement reasonable data security measures because it was foreseeable that PowerSchool's databases would be targeted by hackers given the prominence of security breaches in educational institutional settings, and because it knew of numerous, other well-publicized data breaches and the risks of attempts at unauthorized access to the vast quantities of valuable data held by Defendant(s). Any purported safeguards that Defendants had in place were wholly inadequate.

784. In addition, Defendants had an independent duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which 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.

785. Defendants also had independent duties under Plaintiffs' and Class Members' state laws that required Defendants to reasonably safeguard Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" under federal and state laws are untethered to any contract between Defendants, Plaintiffs, and/or Class Members.

786. Because Defendants knew that a breach of PowerSchool's systems could damage thousands or even millions of individuals, including Plaintiffs and Class Members, Defendants had a duty to adequately protect the relevant data systems and the PII contained therein.

787. Defendants, and each of them, through their actions and/or omissions, breached the duties owed to Plaintiffs and Class Members. Accordingly, Defendants were negligent.

788. Defendant PowerSchool breached its duties by, among other things: (a) failing to adopt, implement, and maintain adequate data security measures and practices to safeguard Plaintiffs' and Class Members' PII; (b) failing to implement and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach; (c) failing to implement multifactor authentication; (d) failing to implement the principle of least privileges; (e) failing to implement the principle of network segmentation; (f) failing to implement rate limiting; (g) failing to secure the contractor's credentials; (h) failing to monitor its logs for unusual activity; (i) failing to adequately implement an intrusion detection and prevention system; (j) failing to encrypt the Data; (k) failing to comply with – and thus violating – e.g., the FTC Act, HIPAA, COPPA, FERPA, and other applicable federal and state laws and regulations; (l) failing to heed industry warnings and alerts to provide adequate safeguards to protect Plaintiffs' and Class Members' PII in the face of increased risk of theft; (m) violating

its duty to exercise appropriate clearinghouse practices by failing to remove PII that was no longer required to be retained; (n) failing to implement processes to detect the Data Breach in a timely manner, and to act upon any related warnings or alerts that its systems were breached; (o) allowing unauthorized access to Plaintiffs' and Class Members' PII; (p) failing to adopt and/or utilize mitigation policies and procedures; and (q) failing to disclose that Defendant's data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

789. In addition to the subparts above, Defendant Movate breached its non-delegable duties to Plaintiffs and Class Members to, among other things: (a) appropriately train its employees and agents to secure their credentials; (b) rotate its employees' and agents' credentials; and (c) and implement the principle of least privileged for data access.

790. PowerSchool also breached its duties by failing to provide adequate and timely notice of the Data Breach to Plaintiffs and Class Members so that they could take appropriate steps to mitigate damages, protect against adverse consequences, and thwart or minimize future misuse of their PII. Instead, PowerSchool waited ten days after learning of the Data Breach to provide notification to Plaintiffs and Class Members and then by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach. This delay only exacerbated Plaintiffs' and Class Members' injuries.

791. To date, PowerSchool still has not provided sufficient information to Plaintiffs and Class Member regarding the extent of the unauthorized access and continue to breach its disclosure obligations to Plaintiffs and Class Members.

792. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risk and known threats.

793. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of the Plaintiffs and Class Members would not

have been compromised. Defendants' negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and Class Members' PII.

794. There is a close causal connection between Defendants' failures to implement security measures to protect the PII of Plaintiffs and the Class Members and the harm – or risk of imminent harm – suffered by Plaintiffs and the Class Members. As a result of Defendants' negligence, the PII of and other sensitive information of Plaintiffs and Class Members was compromised, placing them at greater risk of identity theft, and disclosure of their PII to third parties without their consent.

795. Defendants' negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injuries-in-fact, and damages. These damages and injuries, which were a proximate, reasonably foreseeable result of Defendants' breaches of its duties include, but are not limited to: (a) actual identity theft, fraud, and other misuse; (b) the loss and diminution in value of their privacy and confidentiality of the stolen PII; (c) the risk of compromise, publication, and/or theft of their PII, including illegal sales on the black market; (d) the imminent and impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals; (e) increased incidents of phishing emails and spam calls, texts, and/or emails; (f) mitigation expenses associated with detection, prevention, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (g) out-of-pocket costs associated with purchasing credit monitoring and identity theft prevention services; (h) time spent on exploring or obtaining credit monitoring, identity theft insurance, and credit freezes and unfreezes and other matters related to the Data Breach; (i) expenses and time spent initiating fraud alerts; (j) decreased credit scores and ratings; (k) lost work time; (l) the diminished value of the services Plaintiffs and Class Members paid for and received; (m) continued risk of exposure to hackers and thieves of their PII, which may remain in PowerSchool's possession and is subject to further unauthorized disclosure so long as Defendants fail to undertake appropriate

and adequate measures to protect Plaintiffs' and Class Members' data; and (n) the outlay of costs in terms of time, effort, and money that has been and will continue to be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

796. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. Moreover, injuries-in-fact and damages are ongoing, present, and continuing.

797. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to compensatory, consequential, and/or nominal damages, in an amount to be proven at trial.

798. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) train and supervise employees and agents regarding credentials and rotate credentials, and implement principle of least privileges; and (iv) provide lifetime adequate credit and identity monitoring and other monitoring services to all Plaintiffs and Class Members.

COUNT II – NEGLIGENCE PER SE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR ALTERNATIVELY,ON BEHALF OF PLAINTIFFS AND THE STATEWIDE SUBCLASSES)

(AGAINST DEFENDANTS POWERSCHOOL AND BAIN CAPITAL)

799. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

800. Plaintiffs separately state their claim for negligence based on negligence per se to put Defendants on notice that they intend to seek such a presumption.

801. PowerSchool solicited, collected, stored, and maintained Plaintiffs' and Class Members' PII as part of its regular business activities, which affect commerce.

802. Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, COPPA, FERPA, industry standards, and the various state consumer protection statutes discussed herein are independent sources of PowerSchool's duty to use reasonable data security measures to protect Plaintiffs' and Class Members' PII.

803. The relevant requirements imposed by Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, COPPA, FERPA, industry standards, and state statutory laws inform PowerSchool's duty of care.

804. 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.

805. 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 and secure sensitive consumer data, here, Plaintiffs' and Class Members' PII. The FTC publications and orders described herein also form part of the basis of PowerSchool's duty in this regard.

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

807. PowerSchool also has a duty to use reasonable data security measures under HIPAA. HIPAA was enacted to establish a set of standards and requirements for the transmission of certain health information. 45 C.F.R. § 160.103(3). HIPAA requires covered entities and their business associates, like PowerSchool and Movate, to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA. HIPAA also specifically requires "administrative, physical, and technical safeguards that reasonably and appropriately protect [PII]." Id.

808. PowerSchool further has a duty "to require that [its] business associates comply with HIPAA regulations" and are themselves "responsible for the noncompliance of [its] business associate." 45 C.F.R. § 162.923(e).

809. PowerSchool violated its duty under HIPAA by failing to, or contracting with vendors, like Movate, that failed to, use reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' PII.

810. Further, pursuant to COPPA, 15 U.S.C. § 312.10, PowerSchool had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected,'" and thereafter had a duty to "delete [children's personal information] using reasonable

measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

811. PowerSchool violated COPPA § 312.10 by failing to use reasonable measures to protect PII and not complying with industry standards.

812. Additionally, pursuant to Family Educational Rights and Privacy Act ("FERPA"), see, 20 U.S.C. § 1232(g); 34 CFR Part 99 – a federal law aimed at protecting the privacy of student education records and applies to schools and other educational institutions that receive federal funds –PowerSchool had a duty to adopt reasonable measures to protect certain sensitive student records from being disclosed without the student's consent or knowledge.

813. PowerSchool violated FERPA by failing to adopt reasonable measures to protect the PII it collected, which included confidential student records of Plaintiffs and Class Members, from unauthorized access or disclosure to third parties.

814. PowerSchool's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because basic industry standards require PowerSchool to protect such confidential PII.

815. PowerSchool breached its duty to secure and safeguard Plaintiffs' and Class Members' PII by violating statutory laws, along with industry standards, requiring it to implement and maintain adequate data security to safeguard consumers' personal information.

816. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTC Act, HIPAA Privacy and Security Rules, COPPA, FERPA, industry standards, and state consumer protection statues were intended to protect.

817. The harm that has occurred as a result of PowerSchool 's conduct is the type of harm that the FTC Act, HIPAA Privacy and Security Rules, COPPA, FERPA, industry standards, and state consumer protection statutes were intended to guard against.

818. Indeed, the FTC has pursued numerous enforcement actions against businesses, like PowerSchool, which, as a result of their failure to employ reasonable data security measures, caused the same types of harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

819. It was reasonably foreseeable to PowerSchool that its failure to implement and maintain adequate data security practices to safeguard and protect Plaintiffs' and Class Members' PII would result in the improper access and disclosure of that sensitive information to unauthorized third parties.

820. PowerSchool's conduct is especially egregious given the nature and amount of PII it solicits, collects, stores, and maintains, including on behalf of a significantly large and vulnerable population of minors and children, including those under the age of 13, that substantial damages would result to Plaintiffs and Class Members in the event of a data breach.

821. Had Plaintiffs and Class Members known that PowerSchool did not adequately protect their PII, Plaintiffs and Class Members would not have entrusted PowerSchool with their PII.

822. But for PowerSchool's wrongful and negligent breach of its duties, Plaintiffs and Class Members would not have been injured.

823. PowerSchool's various violations and its failure to comply with applicable laws, including but not limited to, Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, COPPA, FERPA, industry standards, and state consumer protection statutes, constitutes negligence per se.

824. As a direct and proximate result of PowerSchool's negligence per se, Plaintiffs and Class Members have suffered and will suffer injuries and damages, including, but not limited to: (a) actual identity theft, fraud, and other misuse; (b) the loss and diminution in value of their privacy and confidentiality of the stolen PII; (c) the compromise, publication, and/or theft of their PII, including illegal sales on the

black market; (d) the imminent and impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals; (e) mitigation expenses associated with detection, prevention, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (f) out-of-pocket costs associated with purchasing credit monitoring and identity theft prevention services; (g) time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (h) expenses and time spent initiating fraud alerts; (i) decreased credit scores and ratings; (j) lost work time; (k) the diminished value of the services Plaintiffs and Class Members paid for and received; (l) continued risk of exposure to hackers and thieves of their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosure so long as PowerSchool fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and (m) the outlay of costs in terms of time, effort, and money that has been and will continue to be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

825. As a direct and proximate result of PowerSchool's negligence per se, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. Moreover, injuries-in-fact and damages are ongoing, present, and continuing.

826. As a direct and proximate result of PowerSchool's negligence per se, Plaintiffs and Class Members are entitled to compensatory, consequential, and/or nominal damages, in an amount to be proven at trial.

827. Plaintiffs and Class Members are also entitled to injunctive relief requiring PowerSchool to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii)

provide adequate credit and identity and other monitoring services to all Plaintiffs and Class Members.

COUNT III – UNJUST ENRICHMENT

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR ALTERNATIVELY,

ON BEHALF OF PLAINTIFFS AND THE STATEWIDE SUBCLASSES)

(AGAINST DEFENDANTS POWERSCHOOL AND BAIN CAPITAL)

828. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

829. Plaintiffs and Class Members conferred an equitable, legal, and monetary benefit on Defendant. They conferred benefits on Defendants by utilizing their products and services sold to the school districts for valuable consideration and by providing Defendants with their valuable PII. In exchange, Plaintiffs and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have had their PII protected with adequate data security.

830. Upon information and belief, Defendants fund their data security measures entirely from its general revenues, including monetary payments made on behalf of Plaintiffs and Class Members.

831. Defendants were paid a certain sum of money, some of which should have been used to fund appropriate data security measures to have been implemented by Defendants.

832. A portion of the payment made on behalf of Plaintiffs and Class Members was to be used to provide a reasonable and adequate level of data security, and the amount of the portion of each payment made that was allocated to data security is known to PowerSchool.

833. There is a direct nexus between the monies paid to PowerSchool and the requirement that PowerSchool keep Plaintiffs' and Class Members' PII confidential and protected.

834. Protecting the PII of Plaintiffs and Class Members is integral to PowerSchool's business. Without their data, PowerSchool would be unable to provide the business services, software licensing, data processing, and consulting which comprise Defendant's core business.

835. Plaintiffs' and Class Members' data and PII have monetary value.

836. PowerSchool knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

837. PowerSchool failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully provide the product and service for which they were paid or for the value that their PII provided.

838. PowerSchool acquired the Plaintiffs and Class Members' PII through inequitable means in that it failed to implement and disclose the inadequate data security practices alleged.

839. If Plaintiffs and Class Members had known that PowerSchool would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII to PowerSchool or utilized products or services from PowerSchool.

840. PowerSchool enriched itself by saving the costs PowerSchool reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Rather than providing a reasonable level of security that would have prevented the Data Breach, PowerSchool instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by using cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered a direct and

proximate result of PowerSchool's decision to prioritize its own profits over the requisite of data security and the safety of Plaintiffs' and Class Members' PII.

841. PowerSchool's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' PII, while at the same time failing to maintain that information secure from unauthorized access by hackers and identity thieves.

842. There is no justification for PowerSchool's enrichment. It would be inequitable, unfair, unconscionable, and unjust for PowerSchool to be permitted to retain these benefits because the benefits were procured because of and by means of their wrongful conduct.

843. Under the principles of equity and good conscience, PowerSchool should not be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it, including any and all monies belonging to Plaintiffs and Class Members because PowerSchool failed to implement appropriate data management and security measures.

844. Plaintiffs and Class Members have no adequate remedy at law.

845. Each Defendant has not yet implemented adequate protections to prevent a future data breach, nor has it given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm.

846. The equitable relief under the UCL and also creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendants' services). Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially narrow or even eliminate the possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

847. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, in the absence of completed discovery regarding class certification and merits, forcing an election of remedies at the initial pleadings stage is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

848. Under the principles of equity and good conscience, the PowerSchool should not be permitted to retain the benefits, including the monetary payments made and/or the full value of Plaintiffs' and Class Members' PII, because PowerSchool failed to implement appropriate data management and security measures as mandated by common law and statutory duties.

849. Plaintiffs and Class Members are entitled to restitution and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by PowerSchool from its wrongful conduct. This can be accomplished by disgorging into a common fund or establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

850. Thus PowerSchool should be compelled to disgorge their profits and/or proceeds that they unjustly received as a result of maintaining inadequate security to protect the Plaintiffs' and Class Members' PII.

COUNT IV - INVASION OF PRIVACY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR ALTERNATIVELY,
ON BEHALF OF PLAINTIFFS AND THE STATEWIDE SUBCLASSES)
(AGAINST DEFENDANTS POWERSCHOOL AND BAIN CAPITAL)

851. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

852. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties or disclosure for any improper purpose.

853. The reasonableness of this expectation is reflected in longstanding customs and practice; available and widely known security measures intended to prevent unauthorized access to personal information, including information concerning young children and state, federal, and international laws protecting the educational privacy of students and minors. Specifically, these expectations stemmed from PowerSchool's own privacy policies, data privacy agreements, service agreements, guidelines, statements, and affirmative representations, along with societal expectations and public policy, as well as state and federal statutes and regulations including the FTC Act, HIPAA, COPPA and FERPA regulations.

854. Individuals also maintain a reasonable expectation of privacy when they are using products in a compulsory environment such as public schools.

855. Plaintiffs and the Class disclosed their sensitive and confidential PII to PowerSchool, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

856. PowerSchool owed a duty to Plaintiffs and Class Members to keep their PII confidential.

857. PowerSchool failed to protect and allowed unknown and unauthorized third parties to access the PII of Plaintiffs and Class Members.

858. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members would be highly offensive to a reasonable person.

859. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to the reasonable person. PowerSchool intentionally violated Plaintiffs' and Class Members' privacy by choosing to implement low-budget security measures with absolute disregard of its consequences and while simultaneously holding itself out to Plaintiffs and Class Members as respecting a higher standard of security.

860. PowerSchool acted with reckless disregard for the privacy of Plaintiffs and Class Members rising to the level of: (a) an intentional intrusion by Defendants; (b) into a matter that Plaintiffs and Class Members have a right to keep private (i.e., their PII); and (c) which is highly offensive to a reasonable person. Thus, the unauthorized acquisition and theft by a third party of Plaintiffs' and Class Members' PII is highly offensive to the reasonable person.

861. PowerSchool knew or acted with reckless disregard of the fact that organizations handling personally identifiable information are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

862. PowerSchool acted knowingly when it permitted the Data Breach to occurs; it had actual knowledge that its information security practices were inadequate and insufficient.

863. PowerSchool unlawfully invaded the privacy rights of Plaintiffs and Class Members by: (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) leaving their PII exposed to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) leaving their PII exposed to unauthorized parties without the informed and clear consent of Plaintiffs and Class Members. This invasion into the privacy of Plaintiffs and Class Members is serious and substantial.

864. PowerSchool was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' data and PII.

865. PowerSchool acted with such reckless disregard as to the safety of Plaintiffs' and Class Members' PII to rise to the level of intentionally allowing the intrusion upon Plaintiffs' and Class Members' seclusion.

866. In failing to protect Plaintiffs' and Class Members' PII, PowerSchool acted with intentional malice, oppression, and in conscious disregard of Plaintiffs' and Class Members' rights because it knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

867. PowerSchool violated Plaintiffs' and Class Members' right to privacy under the common law, as well as under state and federal law, including FTC Act, HIPAA, COPPA, and FERPA regulations. Plaintiffs and Class Members could not reasonably expect that PowerSchool would commit acts in violation of federal and state civil laws rendering them highly offensive behavior.

868. PowerSchool's conduct would be highly offensive to a reasonable person, particularly given PowerSchool's extensive privacy policy misrepresentations and

false public statements regarding its commitment to user privacy and given that Defendants design products to be used by and to collect PII about children, including young children. The manner of invasion – collection through students' use of education tools and platforms in a compulsory setting – was also highly offensive.

869. Defendants also acted with a knowing state of mind when it intentionally concealed from and delayed notifying Plaintiffs and Class Members in a timely fashion that their PII was disclosed and/or exfiltrated in the Data Breach, thereby materially impairing their mitigation efforts.

870. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiffs' and Class Members' PII has been disclosed, viewed or is at imminent risk of being viewed, is now available for redisclosure without authorization, and their reasonable expectations of privacy in their PII has been intruded upon and frustrated, thereby causing Plaintiffs and Class Members undue harm.

871. Plaintiffs and Class Members have suffered injury by the invasion of their privacy and are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial .

COUNT VI – DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFFS AND THE STATEWIDE SUBCLASSES) (AGAINST ALL DEFENDANTS)

872. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

873. Under the Declaratory Judgment Act, 28 U.S.C.§§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relation of the parties and granting further necessary relief. Furthermore, the Court has broad authority to

restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

874. As previously alleged, PowerSchool owes a duty of care to Plaintiffs and Class Members that requires them to adequately secure and protect Plaintiffs' and Class Members' PII from unauthorized access and disclosure.

875. As previously alleged, Movate owes a duty of care to Plaintiffs and Class Members to hire competent employees and agents and train and supervise them regarding securing credentials, rotating employees' credentials, and implementing the principle of least privileges.

876. Upon information and belief, PowerSchool still possesses Plaintiffs' and Class Members' PII.

877. Upon information and belief, Movate continues to employ employees and agents that are not properly supervised, retained, and trained in adequate data security measures, putting at continued risk Plaintiffs' and Class Members' PII.

878. PowerSchool failed to fulfill its legal duties to secure and safeguard Plaintiffs' and Class Members' PII.

879. Movate failed to fulfill its legal duties to secure and safeguard Plaintiffs' and Class Members' PII.

880. An actual controversy has arisen in the wake of the Data Breach regarding Defendants PowerSchool's and Movate's respective present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' PII, and whether PowerSchool and Movate are currently maintaining data security measures and implementing policies and practices adequate to protect Plaintiffs and Class Members from future data breaches that compromise their PII. Plaintiffs and Class Members remain at imminent risk of further compromise of their PII will occur in the future.

881. Since the Data Breach, PowerSchool has not announced what specific and verifiable steps it has taken to correct the data security infrastructure, processes, or procedures and to remedy the vulnerabilities or deficiencies, including vendor management, that permitted the Data Breach to occur and go undetected, and thereby prevent future attacks.

882. There is no reason to believe that PowerSchool's or Movate's employee training and security measures are any more adequate now than they were before the Data Breach.

883. In fact, now that Defendants' inadequate data security or security monitoring vulnerabilities is known to hackers, PII in PowerSchool's possession is even more vulnerable to cyberattacks.

884. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: a) PowerSchool owes a legal duty to secure users' PII and to timely notify users of a data breach under the common law, Section 5 of the FTC Act, HIPAA, COPPA, FERPA, and various state statutes; and b) PowerSchool's existing data security measures, including vendor management, do not comply with its contractual obligations and breach its legal duty of care to adequately secure Plaintiffs' and Class Members' PII; c) Movate's existing policies and practices regarding employee and agent hiring, training, and supervision around data security and credentials are inadequate and breach its legal duty of care to Plaintiffs' and Class Members' PII; and d) as a result of PowerSchool's and Movate's ongoing breach of this legal duty, Plaintiffs and Class Members remain subject to continuing and imminent risk of extortion and other harms.

885. Further, pursuant to its authority under the Declaratory Judgment Act, this Court should enter judgment declaring that PowerSchool implement and maintain reasonable security measures, including but not limited to the following:

i. Requiring PowerSchool to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;

ii. Engaging third-party security auditors, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on PowerSchool's systems on a periodic basis, and ordering PowerSchool to promptly correct any problems or issues that are detected;

iii. Engaging third-party security auditors, as well as internal security personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of PowerSchool's systems;

vi. Requiring PowerSchool to delete, destroy, and purge the PII of Plaintiffs and Class Members that is not necessary for its provisions of services and unless PowerSchool can provide reasonable justification for the retention of such information when weighed against the privacy interests of Plaintiffs and Class Members;

vii. Conduct regular database scanning and security checks;

viii. Implementing mechanisms, procedures, and vendor management policies to adequately oversee the data security of any companies that PowerSchool contracts with and with which it entrusts highly sensitive personal information, including, but not limited to, Plaintiffs' and Class Members' PII;

ix. Requiring PowerSchool to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII;

x. Mandating the proper notice be sent to all affected consumers, and posted publicly; and

xi. Requiring all further corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

886. Further, pursuant to its authority under the Declaratory Judgment Act, this Court should enter judgment declaring that Movate implement and maintain reasonable security measures, including but not limited to the following:

i. Require that Movate appropriately train its employees and agents to secure their credentials;

ii. Rotate its employees' and agents' credentials; and

iii. Implement the principle of least privileges.

887. This Court should also issue prospective injunctive relief requiring Defendants, and each of them, to employ adequate security practices consistent with law and industry standards to protect users' PII.

888. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate remedy, in the event of another data breach on PowerSchool's systems. The risk of another such breach is real, immediate, and substantial.

889. If another breach of PowerSchool's store of student, parent, and employee data occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

890. Defendants have not yet implemented adequate protections to prevent a future data breach, nor have they given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm.

891. Injunctive relief is also necessary to prevent the members of general public from being misled by Defendants' misrepresentations regarding privacy and security of information and also to implement the necessary security measures to protect the information that may later be in Defendants' possession.

892. Injunctive relief would also ensure and provide Plaintiffs and the public with the ability to control the access to their information, and limit the unnecessary exposure of their PII – data Defendants continue to retain, even when it is no longer needed for any transactions with Plaintiffs.

893. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to PowerSchool and Movate if an injunction is issued. Plaintiffs and Class Members will likely be subjected to a heightened, substantial, imminent risk of fraud, identity theft, and other harms described herein. On the other hand, the cost to PowerSchool and Movate of complying with an injunction by employing reasonable prospective data security measure is relatively minimal, and PowerSchool and Movate have a pre-existing legal obligation to employ such measures.

894. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach on PowerSchool's systems, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

COUNT VII – BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR ALTERNATIVELY,
ON BEHALF OF PLAINTIFFS AND THE STATEWIDE SUBCLASSES)
(AGAINST DEFENDANTS POWERSCHOOL AND BAIN CAPITAL)

895. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

896. By accepting, taking possession, collecting, storing, and processing Plaintiffs' and Class Members' highly sensitive data, Defendants formed a special relationship and became a guardian of Plaintiffs' and Class Members' PII.

897. Defendants became a fiduciary where, as alleged herein, it specifically contracted with its educational entity clients to protect the highly sensitive personal information of the class of potential claimants at issue here – i.e., the students, parents, teachers, and employees of said educational entity clients – who entered their PII into Defendant's software, systems, and databases.

898. Further, Plaintiffs' and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual ongoing fraudulent activity to obtain a new number.

899. Plaintiffs and Class Members provided their PII to Defendants with the understanding that it would be protected and that such PII would not be disseminated to any unauthorized third parties. Plaintiffs and Class Members would not have entrusted Defendants to retain their PII had they known of Defendant's inadequate data security practices.

900. Defendants knew that Plaintiffs and Class Members were relying on Defendants to safeguard and accepted that trust and confidence when it accepted PII from Plaintiffs and Class Members.

901. As a result of that special relationship, Defendants were provided with and stored Plaintiffs' and Class Members' PII, which Defendants were required by law and industry standards to maintain in confidence.

902. Defendants thus had a fiduciary duty to act primarily for Plaintiffs and Class Members, (a) for the safeguarding of Plaintiffs' and Class Members' PII; (b) to timely notify Plaintiffs and Class Members of a Data Breach; and (c) to maintain complete and accurate records of what information Defendants store and where they store it.

903. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. Defendants

breached that duty by failing to properly secure and protect Plaintiffs' and Class Members' PII.

904. Defendant further breached its duty to Plaintiffs and Class Members by failing to implement multi-factor authentication, stricter password, and credential information, along with failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII.

905. Defendants also breached its fiduciary duty to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

906. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members. But for Defendants' breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

907. As a direct and proximate result of Defendants' breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer numerous forms of injury and/or harm, and other economic and non-economic losses as described *supra*.

COUNT IX – NEGLIGENT TRAINING AND SUPERVISION
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

(AGAINST DEFENDANTS POWERSCHOOL AND BAIN CAPITAL))

908. Plaintiffs repeat and reallege the allegations set forth in the Statement of Facts as if fully set forth herein.

909. At all times relevant hereto, Defendants owed a duty to Plaintiffs and Class Members to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their customers.

910. PowerSchool outsourced and hired various subcontractors, including Movate, to provide troubleshooting and technical support, customer service, assistance

with network operations, and configure online platforms, websites, and student information systems. As a subcontractor, Movate's employees and agents have access to highly sensitive and confidential data stored on PowerSchool's SIS, including the Private Information of Plaintiffs and Class Members. Moreover, many of these employees and agents were employed and working off-shore, outside of the United States.

911. PowerSchool owed non-delegable duties to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their Private Information in PowerSchool's possession, custody, or control. PowerSchool granted Movate access to Plaintiffs' and Class Members' Private Information without properly: (a) inquiring about, investigating, or monitoring Movate's data security practices; (c) outsourcing and hiring Movate notwithstanding its operations from remote locations outside of the United States, including the Philippines; (e) requiring Movate to utilize appropriate security measures to protect the confidential information of Plaintiffs and Class Members; and/or (f) ensuring that Movate utilized best practices to protect the confidential natures of Plaintiffs' and Class Members' Private Information.

912. PowerSchool further owed non-delegable duties to Plaintiffs and Class Members to ensure that its employees were properly trained to implement protocols and procedures sufficient to meet at a minimum, industry standards to protect the Private Information of Plaintiffs and Class Members.

913. Defendant Movate, acting as PowerSchool's agent, owed non-delegable duties to Plaintiffs and Class Members to hire competent employees and agents and to train and supervise them to ensure they recognize the duties owed to Plaintiffs and Class Members. Further, having been granted unfettered access to millions of students' and teachers' sensitive data, Movate likewise had a duty to take reasonable steps to ensure adequate data security procedures and practices sufficient to maintain confidential the Private Information.

914. Defendants had a duty to prevent foreseeable harm to others, including Plaintiffs and Class Members, who were the foreseeable and probable victims of any inadequate security practices. Defendants in fact, knew that its failure to protect Plaintiffs' and Class Members' Private Information would likely harm them because it knew that hackers routinely attempt to steal such information and use it for nefarious purposes.

915. Defendants were on notice of the importance of data security due to the abundance of information about risks of inadequate security, not the least of which was previously high publicized data breaches against education institutions.

916. It was reasonably foreseeable that Movate's failure to train employees and agents about the importance of protecting their passwords, failure to require credential changes at regular intervals (e.g., 90 days), and not providing restricted access would compromise the security of Plaintiffs' and Class Members' Private Information.

917. PowerSchool was negligent and failed to exercise the requisite standard of care in the hiring, supervision of its own employees and in its retention of Movate – whose inadequate data security, training, procedures, and network infrastructures – along with its own failures in hiring and training employees and agents – led to the Data Breach and caused the damages suffered by Plaintiffs and Class Members as alleged herein.

918. PowerSchool breached its duty to Plaintiffs and Class Members by failing to ensure that it and Movate employed adequate data security measures, protocols, and practices to protect Plaintiffs' and Class Members Private Information from unauthorized disclosure.

919. Movate was negligent and failed to exercise the requisite standard of care in hiring, supervision, retention, and training of its employees and agents – whose inadequate data security, training, procedures, protocols, and network infrastructure led

to the Data Breach and caused the damages suffered by Plaintiffs and Class Members as alleged herein.

920. Movate breached its duty to Plaintiffs and Class Members by failing to, among other things: (1) appropriately train its employees to secure their credentials; (2) rotate its employees' credentials; (3) and implement the principle of least privileges.

921. Specifically, an individual by the name of Rayson Cruz appears to be a Movate Team Leader who was assigned to provide technical support on behalf of PowerSchool and had access to the PowerSchool Student Information System (again, "SIS"). As a result, his compromised credentials allowed the Data Breach threat actor to exfiltrate Plaintiffs' and Class Members' Private Information.

922. As a direct result of PowerSchool breach of its duty to appropriately and reasonably vet, hire, train, and supervise employees and agents – including its outsourced agent, Movate, and also to take security measures to protect from unauthorized disclosure of Plaintiffs' and the Class Members' Personal Information, Plaintiffs and Class Members suffered damages and will suffer injuries, including, without limitation: (a) actual identity theft, fraud, and other misuse; (b) the loss and diminution in value of their privacy and confidentiality of the stolen Private Information; (c) the risk of compromise, publication, and/or theft of their Private Information, including illegal sales on the black market; (d) the imminent and impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; (e) increased incidents of phishing emails and spam calls, texts, and/or emails; (f) mitigation expenses associated with detection, prevention, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (g) out-of-pocket costs associated with purchasing credit monitoring and identity theft prevention services; (h) time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (i) expenses and time spent initiating fraud alerts; (j) decreased credit scores

and ratings; (k) lost work time; (l) the diminished value of the services Plaintiffs and Class Members paid for and received; (m) continued risk of exposure to hackers and thieves of their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosure so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and (n) the outlay of costs in terms of time, effort, and money that has been and will continue to be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

923. As a direct result of Movate's breach of its duty to appropriately and reasonably train and supervise employees and agents, and also to take security measures to protect from unauthorized disclosure of Plaintiffs' and the Class Members' Personal Information, Plaintiffs and Class Members suffered damages and will suffer injuries, including, without limitation: (a) actual identity theft, fraud, and other misuse; (b) the loss and diminution in value of their privacy and confidentiality of the stolen Private Information; (c) the risk of compromise, publication, and/or theft of their Private Information, including illegal sales on the black market; (d) the imminent and impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; (e) increased incidents of phishing emails and spam calls, texts, and/or emails; (f) mitigation expenses associated with detection, prevention, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (g) out-of-pocket costs associated with purchasing credit monitoring and identity theft prevention services; (h) time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (i) expenses and time spent initiating fraud alerts; (j) decreased credit scores and ratings; (k) lost work time; (l) the diminished value of the services Plaintiffs and Class Members received; (m) continued risk of exposure to hackers and thieves of their Private Information, which may remain in Defendant's possession and is subject to

further unauthorized disclosure so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and (n) the outlay of costs in terms of time, effort, and money that has been and will continue to be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

924. As a direct and proximate result of Defendants' negligent hiring, retention, training, and/or supervision of its employees and agents, along with its wrongful actions and/or inaction, and the resulting Data Breach, Plaintiffs and Class Members have suffered injury and are entitled to damages, including compensatory, and/or nominal or other damages in an amount to be proven at trial.

COUNT X – ALABAMA DECEPTIVE TRADE PRACTICES ACT, ALA. CODE § 8-19-1, ET SEQ.
(ON BEHALF OF PLAINTIFFS CHRISTINA ASHLEY HARDWICK AND MINOR STUDENT L.D., VALARIE RENEE RHODEN AND MINOR STUDENT C.A.R., AND THE ALABAMA SUBCLASS)

925. Alabama Plaintiffs Hardwick and Minor Student L.D., Rhoden and Minor Student C.A.R. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

926. Defendants are "persons" as defined by Ala. Code § 8-19-3(5).

927. Plaintiffs and Alabama Subclass members are "consumers" as defined by Ala. Code § 8-19-3(2).

928. Plaintiffs sent pre-suit notice pursuant to Ala. Code § 8-19-10(e) on July 3, 2025.

929. Defendants advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

930. Defendants engaged in deceptive acts and practices in the conduct of trade or commerce in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

931. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

932. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

933. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

934. Defendants' deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Alabama Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Alabama Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Alabama Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Alabama Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Alabama Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties concerning the security and privacy of Plaintiffs' and Alabama Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

935. Defendants' representations and omissions were material because they were likely to and did deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of Plaintiffs' and Class Members' PII.

936. Defendants intended to mislead Plaintiffs and Alabama Subclass members and induce them to rely on their misrepresentations and omissions.

937. Had Defendants disclosed to Plaintiffs and Alabama Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Alabama Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Alabama Subclass members paid without advising Plaintiffs and Alabama Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Alabama Subclass members' PII. Accordingly, Plaintiffs and the Alabama Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

938. Defendants acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and in so doing, recklessly disregarded Plaintiffs' and the Alabama Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

939. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiffs and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for those goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

940. Defendants' deceptive acts and practices caused substantial injury to Plaintiffs and Alabama Subclass members that they could not reasonably avoid and that outweighed any purported benefits to consumers or to competition.

941. Plaintiffs and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages, or (b) statutory damages of $100 for Plaintiffs and for each Alabama Subclass Member; treble damages; restitution; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

COUNT XI - ARIZONA CONSUMER FRAUD ACT, A.R.S. §§ 44-1521, ET SEQ. (ON BEHALF OF PLAINTIFFS ARIZONA TEACHER WILLIAM JEREMIAH TARBUSH AND MINOR STUDENT A.C.T. AND THE ARIZONA SUBCLASS)

942. Arizona Plaintiffs Teacher William Tarbush and Minor Student A.C.T. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

943. Defendants are "persons" as defined by A.R.S. § 44-1521(6

944. Defendants advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

945. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Arizona Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Arizona Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Arizona Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties concerning the security and privacy of Plaintiffs' and Arizona Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Arizona Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Arizona Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

946. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

947. Defendants intended to mislead Plaintiffs and Arizona Subclass members and induce them to rely on their misrepresentations and omissions.

948. Had Defendants disclosed to Plaintiffs and Arizona Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Arizona Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Arizona Subclass members paid without advising Plaintiffs and Arizona Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of

Plaintiffs' and Arizona Subclass members' PII. Accordingly, Plaintiffs and the Arizona Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

949. Defendants acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and in so doing, recklessly disregarded Plaintiffs' and Arizona Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

950. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and Arizona Subclass members have suffered and will continue to suffer injury; ascertainable losses of money or property; and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for those goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

951. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages, restitution, disgorgement, punitive damages, injunctive relief, and reasonable attorneys' fees and costs

COUNT XII – CALIFORNIA CUSTOMER RECORDS ACT ("CCRA"), CAL. CIV. CODE §§ 1798.80, ET SEQ.
(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

952. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

953. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "own, license, or maintain Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

954. Defendants are businesses that own, maintain, and license Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and California Subclass members.

955. Defendant PowerSchool's violations of the CCRA were prepared, directed, and

956. emanated from Defendants' California headquarters and from where PowerSchool maintains its principal corporate offices in California.

957. As businesses that own or license computerized data that includes Personal Information, Defendants were required to notify California residents when

their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, Defendants were required to notify Plaintiffs and California Subclass members of "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

958. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

959. Plaintiffs' and California Subclass members' PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

960. Because Defendants reasonably believed that Plaintiffs' and California Subclass members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

961. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82.

962. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass members suffered damages, as described above.

963. Plaintiffs and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT XIII – VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT

CAL. CIV. CODE § 1798.100 *ET SEQ.* ("CCPA")

(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

964. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

965. Under section 1798.150(a)(1), "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(A)]…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief (including future data breaches or other compromises of his PII that remain in Defendant's possession), and any other relief the court deems proper.

966. The duty of care under CCPA is clearly stated in section 1798.100(e): "A business that collects a consumer's personal information shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized or illiegal access, destruction, use, modification, or disclosure."

967. Under section 1798.140(i), Plaintiffs and California Subclass members are consumers and California residents.

968. PowerSchool is a "business" under section 1798.140(d). PowerSchool, owned by Bain, does business in the State of California and is "organized or operated for the profit of financial benefit of its shareholders or other owners." Further, at all times herein, PowerSchool had annual gross revenues in excess of twenty-five million ($25,000,000) during the relevant calendar year in accordance with section 1798.140(d)(7)(A).

969. PowerSchool "collects" "consumers'" personal information in that it gathers, obtains, receives information, either actively or passively, by consumers who are students, families, guardians, and school employees residing in California.

970. Personal information is defined in Section 1798.81.5(d) and also related sections such as Section 1798.140(v)(1). In conformity with those sections, PowerSchool actively and passively collected, gathered, obtained, received, accessed, stored, and processed unredacted, unencrypted personal information of Plaintiffs and California Subclass members. Specifically, PowerSchool received over the student and teacher education portal(s), along with the PowerSource and other service portals, personal information including, but not limited to: Plaintiffs' first name (or first initial) and last name in combination with their Social Security Number, health histories and medical information (including PHI), dates of birth, addresses, phone numbers, emails, contact information and contact information of family members, guardians, and caregivers, academic information, and other unique identifier information that is reasonably capable of being associated with, or could be linked directly or indirectly, with a particular household.

971. PowerSchool collected, stored, and maintained Plaintiffs and California Subclass Members' PII and PHI in such a format that permitted unauthorized actors to access it.

972. The purpose and means of processing of such personal information, central to PowerSchool's organization, was to help educational entity clients and individual consumer users to maintain their personal, academic, and medical information and to make said information available upon request for their benefit.

973. PowerSchool is a multi-faceted and multi-directional educational business that partners with a diversity of educational clients, private and public schools, school districts, and other institutional clients, along with students, families, guardians, teachers, and staff. In order to meet client needs, PowerSchool customizes and tailors its software, hardware, internet portals, and data handling methodologies, including the format and substance of PII and PHI that is obtained and provided from educational entity clients and individuals and based on client preferences. PowerSchool software services are "scalable" to client preferences to cater to a multitude of school districts and school administration tasks, including registration, attendance, scheduling, compliance reporting, data management, faculty management, and health management.

974. PowerSchool provides a virtual platform intended to streamline and manage educational administration using a cloud storage system containing PII and PHI. PowerSchool participated in determining how PowerSchool's PII and PHI would be processed, such as helping education clients establish ostensibly secure processes for uploading personal, academic, and medical information and ensuring – or here, failing to ensure – secure and authorized only access to this sensitive data.

975. Under section 1798.140(v)(1), Plaintiffs and California Subclass Members' PII and PHI was subject to disclosure, theft, and unauthorized access as a result of the Data Breach. The Data Breach exposed PII and PHI, including, but not limited, name, Social Security numbers, dates of birth, addresses, phone numbers, emails, photo identification, tax information numbers, health histories, and other medical information.

976. The Data Breach occurred as a direct and proximate result of Defendant's failure to maintain and implement reasonable security procedures, practices, and systems for protecting the exposed, highly sensitive PII and PHI. Defendants' failure to monitor and maintain its systems to identify and account for any suspicious activity thus permitted unauthorized actors to access California Subclass members' PII. Defendants' failures also included but were not limited to, omission to appropriately encrypt and redact personal information, follow industry standards, and failure to install appropriate network firewalls.

977. Pursuant to section 1798.150(b), Plaintiffs provided written notice to Defendants, specifying the provisions that Defendants violated, and stated that Defendants have 30 days to cure. Defendants have failed to cure thereby entitling Plaintiffs and California Subclass members to seek actual damages and statutory damages of no less than $100 and up to S750 per customer record subject to the Data Breach as authorized by the CCPA, along with injunctive and declaratory relief.

COUNT XIV–CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE §§ 56, ET SEQ.

(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENT K.J.A. AND K.D.A, AND THE CALIFORNIA SUBCLASS)

978. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

979. Under § 56.10(a) of the Civil Code, "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining authorization."

980. PowerSchool is a business deemed to be a provider of health care, health care service plan, or contractor as defined in Civil Code § 56.10(a), *supra*, and as further defined in Civil Code § 56.06(a).

981. Specifically, PowerSchool is a business that is organized as a support provider for educational entity clients and has among its primary purposes the maintenance of student medical records and protected health information on its software platforms and computer networks. Design of hardware and software reflects its purpose, and necessarily the organizational purpose of the creator of the hardware and software. PowerSchool maintains such medical information to make it available to students, parents, guardians, teachers, educational staff, schools, and school district personnel, and/or providers of health care upon request, and to allow such individuals and clinicians to manage the individual's information, and for diagnosis and treatment.

982. PowerSchool is an education company, that is, a "business" that is to provide support for schools, school districts and individuals (*i.e.,* students, parents, guardians, and employees) by maintaining student medical records on its software platforms and computer networks. For example, Defendants maintain health and immunization records of the students in schools and school districts for which it provides services regarding students' medical history, mental or physical condition, or treatment. Its services are provided to meet the unique needs of students who require health care in order to succeed. To perform its functions to assist the central purpose of schools, school districts, and individuals, PowerSchool uses student medical information and diagnosis and treatment plans of children to assist the diagnoses of

students' medical and health care needs and monitor their progress to ensure they are healthy enough to learn and be safe at school.

983. PowerSchool received said student medical records, including: health care provider names and contact information; health records; visits to health staff; medical history, mental, and physical conditions; vaccination and immunization records; dietary restrictions; special medical considerations and treatments (*i.e.* asthma, diabetes, seizures, etc.); medication schedules; allergies; and other protected health information, directly from schools, school districts, and individuals in order to alert teachers and staff to any urgent or important medical considerations.

984. Schools and school districts maintain student medical records for a variety of reasons. They are authorized to hire "physicians as full-time supervisors of health" and to provide ambulance care. (Ed. Code, §§ 49472, 49474.) They are required to "assess" a child's disabilities; to provide medical care at sports events; and to cooperate with local health officials in preventing communicable diseases. Defendants' educational entity clients and individual users provide healthcare to students and employees such that their purpose of maintaining medical information is thus consistent with their role as a provider of health care.

985. When schools and school districts share this medical information with Defendants for maintaining on its platforms and databases, and also so it can be made available upon request, the California Civil Code § 56 et. seq. standards of confidentiality are triggered.

986. PowerSchool is also a business deemed to be a provider of health care, health care service plan, or contractor as further defined in Civil Code § 56.06(b).

987. Specifically, PowerSchool is a business that offers software to consumers that is designed to maintain medical information in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the

individual's information, or for the treatment, or management of a medical condition of the individual. PowerSchool is a cloud-based education software used by more than 18,000 customers, primarily K-12 educators, to support more than 50 million students, including those with medical conditions and disabilities.

988. PowerSchool is an education company, that is, a "business" that offers software or hardware (including mobile applications) to consumers, including Plaintiffs, Class Members, schools, school districts, and other educational entity clients and individual consumers. PowerSchool markets itself as a business that offers to assist educational organizations and their staff to handle, among other things, core data tasks. At all times relevant herein, PowerSchool purposefully facilitated and executed the transmission between PowerSchool, school entity and education organization, individual students, their families and guardians, and employees, of such medical information contained in medical records, as well as its receipt and maintenance by PowerSchool. This is a central facet of regular operations in schools and school districts nationwide, ranging from garden-variety basic medical care and vaccination histories to more serious health encounters, which must be documented. PowerSchool's organizational purpose was to help its educational entity clients and individuals maintain this medical information for the benefit of students, families, guardians, and employees, and to make the information available upon request for treatment or to manage health care and medical condition needs.

989. Problematic is that the medical information and other protected health information that Defendants maintained on behalf of Plaintiffs and California Subclass members was individually identifiable to those victims. Medical alerts and medical charts are expected to contain the identity of the patient and contact information to relay health care information to them.

990. Plaintiffs and California Subclass members had their individually identifiable "medical information" created, maintained, preserved, stored, abandoned,

destroyed, or disposed of on or through Defendants' software and network at the time of the Data Breach.

991. Defendants violated Civil Code § 56.101 by failing to maintain and preserve the confidentiality of Plaintiffs' and California Subclass members' medical information.

992. In violation of Civil Code § 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and California Subclass members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality. As a result, Plaintiffs' and California Subclass members' confidential information and records were negligently released to hackers in the Data Breach.

993. Defendants never received written authorization from Plaintiffs and Subclass members for disclosure of their medical information to threat actors of the Data Breach and no statutory exceptions for said disclosure apply.

994. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by Civil code § 56.101(c).

995. PowerSchool's has admitted in its Notice of Data Breach that the stolen Data included, "limited medical alert information…and other related information" and multiple affected school districts reported that, "other related information included medical diagnoses (including mental health information) and medical conditions.

996. Plaintiffs, along with California Subclass members, have received Notice of Data Breach correspondence from Defendants and/or their educational institutions stating that Plaintiffs' medical information and PHI was exposed in the Data Breach.

997. That Plaintiffs' medical information taken in the Data Breach was viewed by unauthorized individuals is evidence by the fact that the hackers successfully breached PowerSchool's computer systems, exfiltrated medical information and other

protected health information from Defendants' database, and demanded a ransom based on viewing the stolen data to ascertain its data.

998. Criminal threat actors accessed and viewed, and continue to access and view, Plaintiffs' and California Subclass members' individually identifiable medical information. The Data Breach threat actor gained access to Defendants' SIS data using an "export data manager" customer support tool, PowerSource. PowerSource contains a maintenance access tool that allows PowerSchool engineers to access Customer SIS for ongoing support and to troubleshoot performance issues. Using this tool, the attacker exported the PowerSchool SIS 'Students' and 'Teachers' database tables, which included Plaintiffs' individually identifiable medical records, to a CSV file, which was then stolen. Technological modalities and artificial intelligence can also serve as access and viewing tools and instruments of unauthorized use.

999. The modus operandi of cyberthieves is to do one of three (or some combination of) things with the data: (i) use the confidential information to commit medical fraud, identity theft, or financial fraud; (ii) sell the information on the dark web to parties who will use the information for illicit purpose; and (iii) extort the entity that allowed the breach to occur in the first place by demanding a ransom be paid for the return of the stolen confidential information or to keep the information from being publicly released. Each of the above acts requires the cyber-thieves to access and view the exfiltrated information to determine exactly what information was taken, determine the scope of the data taken, and to assess the value of the information in order to formulate the ransom amount and/or ascertain the value on the black market.

1000. Despite Defendant's ransom payment and purported witnessing of the destruction of the exfiltrated data, threat actors have continued to exploit the stolen data, re-targeting individual school districts (*e.g.*, at least twenty school districts in North Carolina, the North Carolina Department of Public Instruction, and the Toronto District School Board) with renewed extortion demands. On May 14, 2025, a

PowerSchool representative stated: "PowerSchool is aware that a threat actor has reached out to multiple school district customers in an attempt to extort them using data from previously reported December 2024 incident." (*See,* Scott Ikeda, "PowerSchool Confirms Ongoing Cyber Extortion of Individual Schools Despite Ransom Payment," CPO Magazine (May 14, 2025) (https://www.cpomagazine.com/cyber-security/powerschool-confirms-ongoing-cyber-extortion-of-individual-schools-despite-ransom-payment/.) Such an admission reveals, in fact, that such data has not been destroyed, but rather is still in circulation.

1001. Moreover, hackers in their ordinary criminal course will prepare and process stolen data for sale or follow-on use. Here, impacted students, families, guardians, and teachers of the Data Breach have reported their personal identifiable information is now accessible on the dark web.

1002. The fact that subsequent extortion attempts based on data from the Data Breach are occurring several months later indicates the continued and widespread accessibility of that data, including Plaintiffs' and California Subclass members' medical information, to criminal actors, and are otherwise being distributed, and made available on the internet or other "dark" channels on it, *i.e.,* the dark web.

1003. In violation of Civil Code § 56.101(b)(1)(A), Defendants' electronic health record systems or electronic medical record systems failed to protect and preserve the integrity of electronic medical information.

1004. As a direct and proximate result of Defendants' wrongful conduct, actions, inactions, omissions, and want of ordinary care under the CMIA, PowerSchool negligently disclosed and released, without written authorization, Plaintiffs' and California Subclass members' confidential individually identifiable medical information to a third-party criminal, which an unauthorized third-party criminal accessed and viewed, and thereby causing damages to Plaintiffs and California Subclass members.

1005. Defendants also violated Civil Code § 56.36(b) by negligently disclosing and releasing Plaintiffs' and California Subclass members' confidential information in the Data Breach when it failed to implement adequate security protocols to prevent data breaches, or employ industry standard and commercially available measures to mitigate the risks of any data breach or otherwise comply with industry standard data security requirements.

1006. Defendants' wrongful conduct, actions, inactions, omissions, and want of ordinary care violate the CMIA and directly and proximately caused the Data Breach. Plaintiffs and California Subclass members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their medical information; (2) loss of the opportunity to control how their medical information is used; (3) diminution in the value and use of their medical information entrusted to Defendants with the understandings that Defendants would safeguard it against theft and not allow it to be misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misused of their medical information; (5) continued undue risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their medical information being stolen in the Data Breach.

1007. Plaintiffs and California Subclass members were injured and have damages, as described above, from Defendant's negligent release of their medical information in violation of Civil Code §§ 56.36 and 56.101 and accordingly are entitled to relief under Civil Code § 56.36, including actual damages, nominal statutory damages of $1,000, injunctive relief, and attorneys' fees, expenses, and costs.

COUNT XV – INVASION OF PRIVACY: CALIFORNIA CONSTITUTION CAL. CONST., ARTICLE I § 1
(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

1008. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1009. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

1010. The right to privacy in California's Constitution creates a private right of action against private and government entities.

1011. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

1012. Defendants violated Plaintiffs and California Subclass members' constitutional right to privacy by collecting, storing, and disclosing, or preventing from unauthorized disclosure, their personal identifying information and protected health information, which includes their legally protected privacy interest, and for which they had a reasonable expectation of privacy. Disclosure of their PII and PHI was highly

offensive given the highly sensitive nature of the data. Disclosure of their private medical information in particular could cause humiliation to Plaintiffs and California Subclass Members. Accordingly, disclosure of Plaintiffs' and California Subclass members' PII and PHI is an egregious violation of social norms.

1013. Defendants intruded upon Plaintiffs' and California Subclass members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential PII.

1014. Plaintiffs' and California Subclass members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of Defendants lax and inadequate security practices with respect to securely collecting, storing, and using data, as well as preventing the unauthorized disclosure of their PII; (ii) Plaintiffs and California Subclass Members did not consent or otherwise authorize Defendants to disclose their PII to parties responsible for the cyberattack; and (iii) Plaintiffs and California Subclass members could not reasonably expect Defendants would commit acts in violation of laws protecting their privacy.

1015. Moreover, Defendants (i) knew that their information security practices were inadequate and had numerous security vulnerabilities; (2) intentionally, willfully, recklessly, or negligently failed to take adequate and reasonable measures to ensure that their data systems were protected; (iii) knew that their inadequate data security measures would likely result in a breach; and (iv) knew that such a breach would harm Plaintiffs.

1016. As a result of Defendants' actions, Plaintiffs and California Subclass Members have been damages as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation.

1017. Plaintiffs and California Subclass members suffered actual and concrete injury as a result of Defendants' violations of their privacy interests. Plaintiff and California Subclass members are entitled to appropriate relief, including damages to

compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendants' invasions.

1018. Plaintiffs and California Subclass members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendants as a result of their intrusions upon Plaintiffs' and California Subclass members' privacy.

COUNT XVI – CALIFORNIA UNFAIR COMPETITION LAW. CAL. BUS. & PROF. CODE §§ 17200, ET SEQ. (ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

1019. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1020. Defendants are "persons" as defined by Cal. Bus. & Prof. Code §17201.

1021. Defendants violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

1022. Defendant PowerSchool's violations of the UCL were prepared, directed, and emanated from Defendants' California headquarters and from where PowerSchool maintains its principal corporate offices in California.

1023. Defendants' "unfair" acts and practices include:

(a) Defendants' failure to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

(b) Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security after previous cybersecurity incidents. For example, Defendants lacked proper network segmentation, failed to abide by their own governing IT policies requiring firewalls to be installed and monitored and requiring remote access only via corporate-managed solutions, failed to abide by their own policies mandating strong passwords and use of two-factor authentication, failed to comply with best practices governing SIEM requiring firewall events associated with malware to be logged and reported to a centralized location, and failed to comply with PCI DSS. This conduct, which has little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass, whose PII has been compromised.

(c) Defendants' failure to implement and maintain reasonable security measures also contravened legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in the law, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

(d) Defendants' failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers—including Plaintiffs and the California subclass—could not have known about Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused.

(e) Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

1024. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

1025. Defendants' unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and California Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.

1026. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

1027. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property; the premiums and/or price received by Defendants for their goods and services; the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1028. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law and in so doing recklessly disregarded Plaintiffs' and California Subclass members' rights. Defendants (1) represented in their

information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1029. By deceptively storing, collecting, and disclosing their PII, Defendants have taken money or property from Plaintiffs and Class Members. Had Plaintiffs and Class Members known that Defendants would fail to implement reasonable data security polices they would not have provided their PII to Defendants.

1030. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' 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.

COUNT XVII – AIDING AND ABETTING.

CAL. BUS. & PROF. CODE §§17200, ET SEQ.

(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

1031. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1032. As set forth herein, PowerSchool's failure to securely maintain Plaintiffs' and Class Members' PII was "unfair," "unlawful," and "fraudulent" within the meaning of the Cal. Bus. & Prof. Code §§ 17200 et. seq. such that Plaintiffs and Class Members have suffered harm and damages as a result of PowerSchool's conduct in violation of the UCL.

1033. By eliminating PowerSchool's critical workforce and contracting with third-party Movate for their own financial gain, Defendants acted with knowledge that PowerSchool's misrepresentations and/or omissions regarding the security of user PII would be (a) unlawful under current state or federal law; (b) "unfair," in that Defendants' business practice was immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers; and/or (c) fraudulent in that members of the public were likely to be deceived by PowerSchool's misrepresentations and/or omissions.

1034. Defendants Bain and Movate provided substantial assistance and encouragement to PowerSchool's unlawful, unfair, and fraudulent business practices by requiring PowerSchool to cut its critical workforce and move essential operations offshore to be hosted by third parties.

1035. Defendants Bain and Movate's agreements with PowerSchool and maintenance of Plaintiffs' and Class members' PII were substantial factors in causing the unfair, unlawful, and fraudulent business practices to the Plaintiffs and the Class alleged herein.

1036. As a result, Bain and Movate aided and abetted PowerSchool's violation of Cal. Bus. & Prof. Code §§ 17200 et. seq. and are therefore jointly liable with PowerSchool for the relief sought by Plaintiffs and the Class. Plaintiffs and Class Members have lost money and property as a result of the Bain and Movate's conduct, as stated in herein.

COUNT XVIII – CALIFORNIA CONSUMER LEGAL REMEDIES ACT. CAL. CIV. CODE §§ 1750, ET SEQ. (ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

1037. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1038. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

1039. Defendants are "persons" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

1040. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

1041. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or . . . if they are of another."

1042. Plaintiffs and the members of the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

1043. Defendant PowerSchool's violations of the CCLRA were prepared, directed, and emanated from Defendants' California headquarters and from where PowerSchool maintains its

1044. principal corporate offices in California.

1045. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass members in violation of Civil Code § 1770, including, but not limited to, the following:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade when they were not;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

1046. Defendants' representations and omissions were material because they were likely to and did deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1047. Had Defendants disclosed to Plaintiffs and California Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and class members' PII as part of the services Defendants provided and for which Plaintiffs and Class Members paid without advising

Plaintiffs and class members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' PII. Accordingly, Plaintiffs and the California Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1048. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1049. Plaintiffs and the California Subclass have provided notice of their claims for damages to PowerSchool, in compliance with California Civil Code § 1782(a).

1050. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT XIX – CALIFORNIA'S COMPREHENSIVE DATA ACCESS AND FRAUD ACT, CAL. PENAL CODE § 502

(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

1051. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1052. The CDAFA protects Plaintiffs and California Subclass members from "tampering, interference, damage, and unauthorized access to (including the extraction of data from) lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

1053. Plaintiffs' and California Subclass members' electronic devices are "computers, computer systems, and/or computer networks" within the meaning of the CDAFA.

1054. The CDAFA provides Plaintiffs and California Subclass members, owners of computers and data, who suffered as a result of a violation of the CDAFA. Cal. Penal Code § 502(c)(1).

1055. The CDAFA provides that "a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Cal. Penal Code § 502(j).

1056. Defendants violated Cal. Penal Code § 502(a) by, *inter alia*:

(a) "Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section" Cal. Penal Code § 502(c)(6); and

(b) "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network" Cal. Penal Code § 502(c)(7).

1057. Defendant PowerSchool's violations of the CDAFA were prepared, directed, and

1058. emanated from Defendants' California headquarters and from where PowerSchool maintains its

1059. principal corporate offices in California.

1060. As a direct and proximate result of Defendants' violations of the CDAFA, Plaintiffs and California Subclass members were injured and lost money or property; the premiums and/or price received by Defendants for their goods and services; the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1061. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' violations of the CDAFA; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT XX – CALIFORNIA'S PROHIBITION AGAINST DECEIT BY CONCEALMENT, CAL. CIV. CODE § 1710(3)
(ON BEHALF OF PLAINTIFFS DAVID BROWNLEE AND MINOR STUDENT A.B., NICOLE FLICK AND MINOR STUDENT M.C., DAVID ZARATE AND MINOR STUDENT A.Z., ASHLEY WRIGHT AND MINOR STUDENT A.N.B., DOBIE JAMES AUGUST AND MINOR STUDENTS K.J.A. AND K.D.A., AND THE CALIFORNIA SUBCLASS)

1062. California Plaintiffs David Brownlee and Minor Student A.B., Nicole Flick and Minor Student M.C., and David Zarate and Minor Student A.Z., Ashley Wright and Minor Student A.N.B., and Dobie James August and Minor Students K.J.A. and K.D.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1063. Section 1710(3) of the California Civil Code prohibits "suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want to communication of that fact[.]" Cal. Civ. Code § 1710(3).

1064. As detailed above, Defendants failed to disclose and actively concealed information about the material fact that they did not reasonably or adequately secure Plaintiffs and the California Subclass members' PII, as well as the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and PII of the California Subclass members. As Defendants knew, their knowledge was exclusive to themselves and was not generally known to the public or to Plaintiffs and the California Subclass members, and had a duty to disclose those material facts to Plaintiffs and the California Subclass members.

1065. Defendants knew that the security of the PII of Plaintiffs and the California Subclass members was materially worse than they represented and what Plaintiffs and the California Subclass members reasonably expected. Defendants

intentionally concealed or suppressed that fact with intent to defraud Plaintiffs and the California Subclass members.

1066. The information Defendants concealed was material in that it was important to reasonable persons, and Plaintiffs and the California Subclass members would not have acted as they did if they had known of the concealed or suppressed fact. As a result, Plaintiffs and the California Subclass members provided PowerSchool with their PII they would not otherwise have provided.

1067. Furthermore, had Plaintiffs and the California Subclass members known of the inadequate privacy and security of Defendants' services, Plaintiffs and the California Subclass members would have taken steps to protect themselves and their personal information.

1068. Plaintiffs and the California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' violations of Section 1710; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief.

COUNT XXI – COLORADO SECURITY BREACH NOTIFICATION ACT, COLO. REV. STAT. §§ 6-1-716, ET SEQ.|
(ON BEHALF OF PLAINTIFF FORMER STUDENT KENNAH J. WHITE AND THE COLORADO SUBCLASS)

1069. Colorado Plaintiff Former Student Kennah J. White ("Plaintiff," for purposes of this Count) repeats and re-alleges the factual allegations above as if fully set forth herein

1070. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

1071. Plaintiff and Colorado Subclass members' PII includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

1072. Under Colo. Rev. Stat. § 6-1-716(2), if Defendants becomes aware of a breach of their data security system, it must—in the most expedient time possible and without unreasonable delay—accurately notify Plaintiff and Colorado Subclass members.

1073. Because Defendants were aware of a breach of their security system, it was obligated to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

1074. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Colo. Rev. Stat. § 6-1-716(2).

1075. As a direct and proximate result of Defendants' violations of Colo. Rev. Stat. § 6-1- 716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

1076. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1- 716(4), including actual damages and equitable relief.

COUNT XXII – COLORADO CONSUMER PROTECTION ACT, COLO. REV. STAT. §§ 6-1-101, ET SEQ. (ON BEHALF OF PLAINTIFF FORMER STUDENT KENNAH J. WHITE AND THE COLORADO SUBCLASS)

1077. Colorado Plaintiff Former Student Kennah J. White ("Plaintiffs," for purposes of this Count) repeats and re-alleges the factual allegations above as if fully set forth herein.

1078. Defendants are "persons" as defined by Colo. Rev. Stat. § 6-1-102(6).

1079. Defendants engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

1080. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Defendants or their successors in interest to actual consumers.

1081. Defendants engaged in deceptive trade practices in the course of their business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

(a) Knowingly making a false representation as to the characteristics of products and services;

(b) Representing that services are of a particular standard, quality, or grade, though Defendants knew or should have known that they were another;

(c) Advertising services with intent not to sell them as advertised; and

(d) Failing to disclose material information concerning their services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

1082. Defendants' deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Colorado Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Plaintiff's and Colorado Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Colorado Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Colorado Subclass members' Personal Information; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1083. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1084. Defendants intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on their misrepresentations and omissions.

1085. Had Defendants disclosed to Plaintiff and Colorado Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Colorado Subclass members' Personal Information as part of the services Defendants provided and for which Plaintiff and Class Members paid without advising Plaintiff and Class Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Colorado Subclass members' Personal Information. Accordingly, Plaintiff and the Colorado Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1086. Defendants acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act and recklessly disregarded Plaintiff's and Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiff's and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1087. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

1088. Defendant PowerSchool's deceptive trade practices significantly affect the public because PowerSchool is the largest student information system in the world, servicing over 60 million students globally in 90 countries, and 90 of the largest 100 school districts in the United States.

1089. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Defendants' bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

COUNT XXIII – FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
FLA. STAT. §§ 501.201, ET SEQ.
(ON BEHALF OF PLAINTIFFS DAVID SAUVE AND MINOR STUDENT A.S. AND THE FLORIDA SUBCLASS)

1090. Florida Plaintiffs David Sauve and Minor Student A.S. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1091. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

1092. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Subclass 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute,

(d) F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

(e) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Florida Subclass members' PII, including by implementing and maintaining reasonable security measures;

(f) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, F.S.A. § 501.171(2);

(g) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Florida Subclass members' PII; and

(h) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

1093. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1094. Had Defendants disclosed to Plaintiffs and Florida Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Florida Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Class Members paid without advising Plaintiffs and Florida Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Florida Subclass members' PII. Accordingly, Plaintiffs and the Florida Subclass members acted

reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1095. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1096. Plaintiffs and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

COUNT XXIV – GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
GA. CODE ANN. §§ 10-1-370, ET SEQ.
(ON BEHALF OF PLAINTIFFS TEACHER CHARLOTTE RENN, KATHERINE STEWART AND MINOR STUDENT R.H.S., AND JOHN RAWLS AND MINOR STUDENT C.R., AND THE GEORGIA SUBCLASS)

1097. Georgia Plaintiffs Teacher Charlotte Renn, Katherine Stewart and Minor Student R.H.S., and John Rawls and Minor Student C.R. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1098. Defendants are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

1099. Defendants engaged in deceptive trade practices in the conduct of their business, in violation of Ga. Code § 110-1-372(a), including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

(c) Advertising goods or services with intent not to sell them as advertised;

(d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

1100. Defendants' deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Georgia Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Georgia Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Georgia Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Georgia Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Georgia Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Georgia Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1101. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1102. Defendants intended to mislead Plaintiffs and Georgia Subclass members and induce them to rely on their misrepresentations and omissions.

1103. In the course of their business, Defendants engaged in activities with a tendency or capacity to deceive.

1104. Defendants acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act and recklessly disregarded Plaintiffs' and Georgia Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1105. Had Defendants disclosed to Plaintiffs and Georgia Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants

could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Georgia Subclass members' Personal Information as part of the services Defendants provided and for which Plaintiffs and Class Members paid without advising Plaintiffs and Class Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Georgia Subclass members' PII. Accordingly, Plaintiffs and the Georgia Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1106. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiffs and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1107. Plaintiffs and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code § 10-1-373.

COUNT XXV – O.C.G.A. § 13-6-11 RECOVERY OF EXPENSES OF LITIGATION (ON BEHALF OF PLAINTIFFS TEACHER CHARLOTTE RENN, KATHERINE STEWART AND MINOR STUDENT R.H.S., AND JOHN RAWLS AND MINOR STUDENT C.R., AND THE GEORGIA SUBCLASS)

1108. Plaintiffs Teacher Charlotte Renn, Katherine Stewart and Minor Student R.H.S., and John Rawls and Minor Student C.R. ("Plaintiffs," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeat and allege TK PARAS, as if fully alleged herein.

1109. Under O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

1110. PowerSchool, through its actions alleged and described herein, acted in bad faith, was stubbornly litigious, or caused Plaintiffs and the Georgia Subclass unnecessary trouble and expense regarding the transaction or events underlying this litigation.

1111. Plaintiffs and the Georgia Subclass therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees under O.C.G.A. § 13-6-11.

COUNT XXVI – IDAHO CONSUMER PROTECTION ACT, IDAHO CODE §§48-601, ET SEQ.

(ON BEHALF OF PLAINTIFF MARY LORENE MUCKELORY AND MINOR STUDENTS D.W.M. AND J.R.M. AND THE IDAHO SUBCLASS)

1112. Idaho Plaintiffs Mary Lorene Muckelory and Minor Students D.W.M. and J.R.M. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1113. Defendants are "persons" as defined by Idaho Code § 48-602(1).

1114. Defendants' conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

1115. Defendants advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

1116. Defendants engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce pertaining to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. Representing that goods are of a particular standard, quality, or grade when they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers; and

e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.

1117. Defendants' unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Idaho Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Idaho Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Idaho Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Idaho Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Idaho Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Idaho Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1118. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1119. Defendants intended to mislead Plaintiffs and Idaho Subclass members and induce them to rely on their misrepresentations and omissions. Defendants knew their representations and omissions were false.

1120. Defendants acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act and recklessly disregarded Plaintiffs' and Idaho Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1121. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable conduct, Plaintiffs and Idaho Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity-protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft

1122. Plaintiffs and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, costs, and attorneys' fees.

COUNT XXVII – ILLINOIS PERSONAL INFORMATION PROTECTION ACT,
815 ILL. COMP. STAT. §§ 530/10(A), ET SEQ.
(ON BEHALF OF PLAINTIFFS JILL STRELZIN AND MINOR STUDENTS J.S. AND R.S., NICOLE VOLPERT AND MINOR STUDENT S.R.V., NICOLE COSENTINO AND MINOR STUDENT C.M.C., AND THE ILLINOIS SUBCLASS)

1123. Illinois Plaintiffs Jill Strelzin and Minor Students J.S. and R.S., Nicole Volpert and Minor Student S.R.V., and Nicole Cosentino and Minor Student C.M.C. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1124. As entities that handle, collect, disseminate, and otherwise deal with nonpublic personal information, Defendants are "Data Collectors" as defined by 815 Ill. Comp. Stat. § 530/5.

1125. Plaintiffs' and Illinois Subclass members' PII includes Personal Information as defined by 815 Ill. Comp. Stat. § 530/5.

1126. As Data Collectors, Defendants were required to notify Plaintiffs and Illinois Subclass members of a breach of their data security system in the most expedient time possible and without unreasonable delay.

1127. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Defendants violated 815 Ill. Comp. Stat. § 530/10(a).

1128. Defendants decisions to fail to timely disclose the Data Breach to Plaintiffs and Illinois Subclass members was knowing and willful.

1129. Under 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

1130. As a direct and proximate result of Defendants' violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiffs and Illinois Subclass members suffered damages, as described above.

1131. Plaintiffs and Illinois Subclass members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Defendants' willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT XXVIII – ILLINOIS CONSUMER FRAUD ACT, 815 ILL. COMP. STAT. §§ 505, ET SEQ. (ON BEHALF OF PLAINTIFFS JILL STRELZIN AND MINOR STUDENTS J.S. AND R.S., NICOLE VOLPERT AND MINOR STUDENT S.R.V., AND NICOLE COSENTINO AND MINOR STUDENT C.M.C. AND THE ILLINOIS SUBCLASS)

1132. Illinois Plaintiffs Jill Strelzin and Minor Students J.S. and R.S., Nicole Volpert and Minor Student S.R.V., and Nicole Cosentino and Minor Student C.M.C. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1133. Defendants are "persons" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

1134. Plaintiffs and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

1135. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

1136. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Illinois Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Plaintiff and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Illinois Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

1137. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1138. Defendants intended to mislead Plaintiffs and Illinois Subclass members and induce them to rely on their misrepresentations and omissions.

1139. Defendants' above-described unfair and deceptive practices and acts were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any purported benefits to consumers or to competition.

1140. Defendants acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act and recklessly disregarded Plaintiffs' and Illinois Subclass members' rights Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1141. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1142. Plaintiffs and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XXIX – ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,
815 ILL. COMP. STAT. §§ 510/2, ET SEQ.
(ON BEHALF OF PLAINTIFFS JILL STRELZIN AND MINOR STUDENTS J.S. AND R.S., NICOLE VOLPERT AND MINOR STUDENT S.R.V., AND NICOLE COSENTINO AND MINOR STUDENT C.M.C. AND THE ILLINOIS SUBCLASS)

1143. Illinois Plaintiffs Jill Strelzin and Minor Students J.S. and R.S., Nicole Volpert and Minor Student S.R.V., and Nicole Cosentino and Minor Student C.M.C. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1144. Defendants are "persons" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

1145. Defendants engaged in deceptive trade practices in the conduct of their business in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade if they are of another;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

1146. Defendants' deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Illinois Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Illinois Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

1147. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1148. Defendants' above-described unfair and deceptive practices and acts were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any purported benefits to consumers or to competition.

1149. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiffs and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1150. Plaintiffs and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT XXX – INDIANA DECEPTIVE CONSUMER SALES ACT, IND. CODE §§ 24-5-0.5-1, ET SEQ.
(ON BEHALF OF PLAINTIFFS TEACHER KIMBERLY KINNEY, AMANDA VOLTZ AND MINOR STUDENTS B.L.C. AND K.D.V., AND THE INDIANA SUBCLASS)

1151. Indiana Plaintiffs Teacher Kimberly Kinney, Amanda Voltz and Minor Students B.L.C. and K.D.V. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1152. Defendants are "persons" as defined by Ind. Code § 24-5-0.5-2(a)(2).

1153. Defendants are "suppliers" as defined by § 24-5-0.5-2(a)(1) because they regularly engage in or solicit "consumer transactions" within the meaning of § 24-5-0.5-2(a)(3)(A).

1154. Defendants engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions in violation of Ind. Code § 24-5-0.5-3(a).

1155. Defendants' representations and omissions include both implicit and explicit representations.

1156. Defendants' unfair, abusive, and deceptive acts, omissions, and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Indiana Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Indiana Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Indiana Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

1157. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers that was not reasonably avoidable by consumers themselves or outweighed by countervailing benefits to consumers or to competition.

1158. The injury to consumers from Defendants' conduct was and is substantial because it was non-trivial, non-speculative, and involved a monetary injury and an unwarranted risk to the safety of consumers' PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a

significant number of consumers but also because it inflicted a significant amount of harm on each consumer.

1159. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1160. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

1161. Defendants' acts and practices were "abusive" for numerous reasons, including:

(a) because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Defendants' failure to disclose the inadequacies in their data security interfered with consumers' decision-making in a variety of their transactions.

(b) because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Defendants' data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

(c) because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Defendants concerning the state of Defendants' data security.

(d) because Defendants took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

1162. Defendants also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

(a) Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

(b) Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if they are not and if the supplier knows or should reasonably know that they are not; and

(c) Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

1163. Defendants intended to mislead Plaintiffs and Indiana Subclass members and induce them to rely on their misrepresentations and omissions.

1164. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1165. Had Defendants disclosed to Plaintiffs and Indiana Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Indiana Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Indiana Subclass members paid without advising Plaintiffs and Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Indiana Subclass members' PII. Accordingly, Plaintiff and the Indiana Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1166. Defendants had a duty to disclose the above-described facts due to the circumstance of this case and the sensitivity and extensiveness of the PII in their possession. This duty arose because members of the public, including Plaintiffs and the Indiana Subclass, repose a trust and confidence in Defendants to keep their PII secure. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Indiana Subclass—and Defendants because consumers cannot fully protect their interests regarding their data and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

1167. Defendants acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act and recklessly disregarded Plaintiffs' and Indiana Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1168. Plaintiffs sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on July 11, 2025. PowerSchool has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

1169. Since Plaintiffs provided the requisite notice, Defendants have failed to cure their violations of the Indiana Deceptive Consumer Sales Act.

1170. Defendants have not cured their unfair, abusive, and deceptive acts and practices, or their violations of Indiana Deceptive Consumer Sales Act are incurable.

1171. Defendants' conduct includes incurable deceptive acts that Defendants engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5- 2(a)(8).

1172. As a direct and proximate result of Defendants' uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiffs and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1173. Defendants' violations present a continuing risk to Plaintiffs and Indiana Subclass members as well as to the general public.

1174. Plaintiffs and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

COUNT XXXI – PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, IOWA CODE § 715C.2 (ON BEHALF OF PLAINTIFFS FORMER STUDENT ALEXANDER LARSON, KYLIE STOWE AND MINOR STUDENT Z.S., AND THE IOWA SUBCLASS)

1175. Iowa Plaintiffs Former Student Alexander Larson and Kylie Stowe and Minor Student Z.S. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1176. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

1177. Plaintiffs' and Iowa Subclass members' PII includes Personal Information as covered under Iowa Code § 715C.2(1).

1178. Pursuant to Iowa Code § 715C.2(1), Defendants were required to accurately notify Plaintiffs and Iowa Subclass members in the most expeditious time possible of the Data Breach without unreasonable delay.

1179. Because Defendants were aware of a breach of its security system, Defendants were obligated to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code§ 715C.2(1).

1180. Defendants violated Iowa Code § 715C.2(1) by failing to disclose the Data Breach in a timely and accurate manner.

1181. Under Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice under Iowa Code Ann. § 714.16(7).

1182. As a direct and proximate result of Defendants' violations of Iowa Code § 715C.2(1), Plaintiffs and Iowa Subclass members suffered damages, as described above.

1183. Plaintiffs and Iowa Subclass members seek relief under Iowa Code § 714.16(7) and Iowa Code§ 715C.2(9)a, including actual damages and injunctive relief.

COUNT XXXII – IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT,
IOWA CODE § 714H
(ON BEHALF OF PLAINTIFFS FORMER STUDENT ALEXANDER LARSON, KYLIE STOWE AND MINOR STUDENT Z.S., AND THE IOWA SUBCLASS)

1184. Iowa Plaintiffs Former Student Alexander Larson and Kylie Stowe and Minor Student Z.S. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1185. Defendants are "persons" as defined by Iowa Code § 714H.2(7).

1186. Plaintiffs and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

1187. Defendants' conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

1188. Defendants engaged in unfair, deceptive, and unconscionable trade practices in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Iowa Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 Iowa Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Iowa Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Iowa Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Iowa Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Iowa Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1189. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1190. Defendants intended to mislead Plaintiffs and Iowa Subclass members and induce them to rely on their misrepresentations and omissions.

1191. Defendants acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act and recklessly disregarded Plaintiffs' and Iowa Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive

personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1192. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable conduct, Plaintiffs and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1193. Plaintiffs have provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit under Iowa Code § 714H.7.

1194. Plaintiffs and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, punitive damages, and reasonable attorneys' fees and costs.

COUNT XXXIII – PROTECTION OF CONSUMER INFORMATION, KAN. STAT. ANN. §§ 50-7A02(A), ET SEQ.
(ON BEHALF OF PLAINTIFFS FORMER STUDENT EMMA PANGRACS, FORMER STUDENT LAUREN OVERLY, SHANDA FARQUHAR AND MINOR STUDENT G.A.F., AND THE KANSAS SUBCLASS)

1195. Kansas Plaintiffs Former Student Emma Pangracs, Former Student Lauren Overly, Shanda Farquhar And Minor Student G.A.F ("Plaintiffs," for purposes

of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1196. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

1197. Plaintiffs' and Kansas Subclass members' PII includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

1198. Under Kan. Stat. Ann. § 50-7a02(a), if Defendants becomes aware of a breach of their data security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, it must—in the most expedient time possible and without unreasonable delay—accurately notify Plaintiffs and Kansas Subclass members.

1199. Because Defendants were aware of a breach of their security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, Defendants were obligated to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

1200. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Kan. Stat. Ann. § 50-7a02(a).

1201. As a direct and proximate result of Defendants' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiffs and Kansas Subclass members suffered damages, as described above.

1202. Plaintiffs and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT XXXIV – KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, ET SEQ.
(ON BEHALF OF PLAINTIFFS FORMER STUDENT EMMA PANGRACS, FORMER STUDENT LAUREN OVERLY, AND SHANDA FARQUHAR AND MINOR STUDENT G.A.F., AND THE KANSAS SUBCLASS)

1203. Kansas Plaintiffs Former Student Emma Pangracs, Former Student Lauren Overly, and Shanda Farquhar and Minor Student G.A.F. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1204. K.S.A. §§ 50-623, et seq. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

1205. Plaintiffs and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

1206. The acts and practices described herein are "consumer transactions" as defined by K.S.A. § 50-624(c).

1207. Defendants are a "supplier" as defined by K.S.A. § 50-624(l).

1208. Defendants advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

1209. Defendants engaged in deceptive and unfair acts or practices, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Kansas Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Kansas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Kansas Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Kansas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Kansas Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Kansas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

1210. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1211. Defendants intended to mislead Plaintiffs and Kansas Subclass members and induce them to rely on their misrepresentations and omissions.

1212. Had Defendants disclosed to Plaintiffs and Kansas Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could

not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Kansas Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Kansas Subclass members paid without advising Plaintiffs and Kansas Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Kansas Subclass members' PII. Accordingly, Plaintiffs and the Kansas Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1213. Defendants also engaged in unconscionable acts and practices in connection with a consumer transaction in violation of K.S.A. § 50-627, including:

(a) Knowingly taking advantage of Plaintiffs' and Kansas Subclass members' inability to reasonably protect their interests due to their lack of knowledge (see K.S.A. § 50- 627(b)(1)); and

(b) Requiring Plaintiffs and the Kansas Subclass to enter into a consumer transaction on terms that Defendants knew were substantially one-sided in favor of itself (see K.S.A § 50-627(b)(5)).

1214. Plaintiffs and Kansas Subclass members had unequal bargaining power regarding their ability to control the security and confidentiality of their PII in Defendants' possession.

1215. Defendants' above-described unfair, deceptive, and unconscionable practices and acts were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any purported benefits to consumers or to competition.

1216. Defendants acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act and recklessly disregarded Plaintiffs' and Kansas

Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1217. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable trade practices, Plaintiffs and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1218. Plaintiffs and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater) under K.S.A. §§ 50-634 and 50-636; injunctive relief; restitution; and reasonable attorneys' fees and costs.

COUNT XXXV – DATABASE SECURITY BREACH NOTIFICATION LAW, LA. REV. STAT. ANN. §§ 51:3074(A), ET SEQ.
(ON BEHALF OF PLAINTIFFS SCOTT GRECI AND MINOR STUDENT L.G., AND TIFFANY HONORE AND MINOR STUDENT M.M., AND THE LOUISIANA SUBCLASS)

1219. Louisiana Plaintiffs Scott Greci and Minor Student L.G. and Tiffany Honore and Minor Student M.M. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1220. Defendants are businesses that own or license computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

1221. Plaintiffs' and Louisiana Subclass members' PII includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

1222. Pursuant to La. Rev. Stat. Ann. § 51:3074(C), Defendants were required to notify Plaintiffs and Louisiana Subclass members of the Data Breach in the most expedient time possible and without unreasonable delay.

1223. Defendants violated La. Rev. Stat. Ann. § 51:3074(C) by failing to disclose the Data Breach in a timely and accurate manner.

1224. As a direct and proximate result of Defendants' violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiffs and Louisiana Subclass members suffered damages, as described above.

1225. Plaintiffs and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT XXXVI – LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,
LA REV. STAT. ANN. §§ 51:1401, ET SEQ.
(ON BEHALF OF PLAINTIFFS SCOTT GRECI AND MINOR STUDENT L.G., AND TIFFANY HONORE AND MINOR STUDENT M.M., AND THE LOUISIANA SUBCLASS)

1226. Louisiana Plaintiffs Scott Greci and Minor Student L.G. and Tiffany Honore and Minor Student M.M. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1227. Plaintiffs, Louisiana Subclass members, and Defendants are "persons" within the meaning of La. Rev. Stat. Ann. § 51:1402(8).

1228. Plaintiffs and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

1229. Defendants engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

1230. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). "Unfair acts" are those that offend established public policy; "deceptive acts" are practices that amount to fraud, deceit, or misrepresentation.

1231. Defendants participated in both unfair and deceptive acts and practices that violated the Louisiana CPL, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Louisiana Subclass members' PII, 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, and adequately improve security and privacy

measures following previous cybersecurity incidents, 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 Louisiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Louisiana Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Louisiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Louisiana Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Louisiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1232. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1233. Defendants intended to mislead Plaintiffs and Louisiana Subclass members and induce them to rely on their misrepresentations and omissions.

1234. Defendants' unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to

Plaintiffs and Louisiana Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1235. Defendants acted intentionally, knowingly, and maliciously to violate the Louisiana CPL and recklessly disregarded Plaintiffs' and Louisiana Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1236. Had Defendants disclosed to Plaintiffs and Louisiana Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Louisiana Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Louisiana Subclass members paid without advising Plaintiffs and Louisiana Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Louisiana Subclass members' PII. Accordingly, Plaintiffs and the Louisiana Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1237. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less

for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1238. Plaintiffs and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Defendants' knowing violations of the Louisiana CPL; restitution; declaratory relief; attorneys' fees; and any other relief that is just and proper.

COUNT XXXVII – MAINE UNFAIR TRADE PRACTICES ACT, 5 ME. REV. STAT. §§ 205, 213, ET SEQ. (ON BEHALF OF PLAINTIFF ZANDER NORCIA AND THE MAINE SUBCLASS)

1239. Maine Plaintiff Zander Norcia ("Plaintiff," for purposes of this Count) repeats and re-alleges the factual allegations above as if fully set forth herein.

1240. Defendants are "persons" as defined by 5 Me. Rev. Stat. § 206(2).

1241. Defendants' conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Rev. Stat. § 206(3).

1242. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes, directly or indirectly.

1243. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) on July 11, 2025.

1244. Defendants engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 Plaintiff's and Maine Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Maine Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maine Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Maine Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maine Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1245. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1246. Had Defendants disclosed to Plaintiff and Maine Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could

not have continued in business and would have been forced to adopt reasonable data security measures

1247. and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Maine Subclass members' PII as part of the services Defendants provided and for which Plaintiff and Maine Subclass members paid without advising Plaintiff and Maine Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Maine Subclass members' PII. Accordingly, Plaintiff and the Maine Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1248. As a direct and proximate result of Defendants' unfair and deceptive acts and conduct, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1249. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

COUNT XXXVIII – MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT,
10 ME. REV. STAT. §§ 1212, ET SEQ.
(ON BEHALF OF PLAINTIFF ZANDER NORCIA AND THE MAINE SUBCLASS)

1250. Maine Plaintiffa Zander Norcia ("Plaintiff," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1251. Defendants are "persons" as defined by 10 Me. Rev. Stat. § 1211(5).

1252. Defendants advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

1253. Defendants engaged in deceptive trade practices in the conduct of their business in violation of 10 Me. Rev. Stat. §1212, including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade if they are of another;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

1254. Defendants' deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Maine Subclass members' PII, 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, and adequately improve security and privacy

measures after previous cybersecurity incidents, 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 Plaintiff and Maine Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Maine Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1255. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1256. Defendants intended to mislead Plaintiff and Maine Subclass members and induce them to rely on their misrepresentations and omissions.

1257. Had Defendants disclosed to Plaintiff and Maine Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data

security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Maine Subclass members' PII as part of the services Defendants provided and for which Plaintiff and Maine Subclass members paid without advising Plaintiff and Maine Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Maine Subclass members' PII. Accordingly, Plaintiff and the Maine Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1258. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1259. Maine Subclass members are likely to be damaged by Defendants' ongoing deceptive trade practices.

1260. Plaintiff and the Maine Subclass members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

COUNT XXXIX – MARYLAND PERSONAL INFORMATION PROTECTION ACT,

MD. COMM. CODE §§ 14-3501, ET SEQ.

(ON BEHALF OF PLAINTIFFS ALYSHA NOBLE AND MINOR STUDENT R.J.S. AND THE MARYLAND SUBCLASS)

1261. Maryland Plaintiffs Alysha Noble and Minor Student R.J.S. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1262. Under Md. Comm. Code § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that own or license Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and their operations."

1263. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

1264. Plaintiffs and Maryland Subclass members are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

1265. Plaintiffs' and Maryland Subclass members' PII includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

1266. Defendants did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information it owned or licensed and the nature and size of their business and operations in violation of Md. Comm. Code § 14-3503.

1267. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

1268. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that own or license computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

1269. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

1270. Because Defendants discovered a security breach and had notice of a security breach, it was obligated under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) to disclose the Data Breach in a timely and accurate fashion.

1271. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

1272. As a direct and proximate result of Defendants' violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Maryland Subclass members suffered damages, as described above.

1273. Under Md. Comm. Code § 14-3508, Defendants' violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101 et seq., and subject to the enforcement and penalty provisions contained within it.

1274. Plaintiffs and Maryland Subclass members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

COUNT XL – MARYLAND CONSUMER PROTECTION ACT, MD. CODE ANN., COM. LAW §§ 13-301, ET SEQ. (ON BEHALF OF PLAINTIFFS ALYSHA NOBLE AND MINOR STUDENT R.J.S. AND THE MARYLAND SUBCLASS)

1275. Maryland Plaintiffs Alysha Noble and Minor Student R.J.S. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1276. Defendants are "persons" as defined by Md. Code, Com Law § 13-101(h).

1277. Defendants' conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Code, Com. Law § 13-101(i) and § 13-303.

1278. Plaintiffs and Maryland Subclass members are "consumers" as defined by Md. Code, Com. Law § 13-101(c).

1279. Defendants advertise, offer, or sell "consumer goods" or "consumer services" as defined by Md. Code, Com. Law § 13-101(d).

1280. Defendants advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

1281. Defendants engaged in unfair and deceptive trade practices in violation of Md. Code, Com. Law § 13-301, including:

(a) Making false or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

(b) Representing that consumer goods or services have a characteristic that they do not have;

(c) Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

(d) Failing to state a material fact where the failure deceives or tends to deceive;

(e) Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

(f) Deception, fraud, false pretense, false premise, misrepresentation or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

1282. Defendants engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services in violation of Md. Code, Com Law § 13-303, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and class members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Plaintiff and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Maryland Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Maryland

Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Maryland Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Maryland Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503.

1283. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII. Defendants' misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

1284. Defendants intended to mislead Plaintiffs and Maryland Subclass members and induce them to rely on their misrepresentations and omissions.

1285. Had Defendants disclosed to Plaintiffs and Maryland Subclass members that their data systems were not secure and were thus vulnerable to attack, could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Maryland Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Maryland Subclass members paid without advising Plaintiffs and Maryland Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Maryland Subclass members' PII. Accordingly, Plaintiffs and the

Maryland Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1286. Defendants acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act and recklessly disregarded Plaintiffs' and Maryland Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1287. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1288. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT XLI – MASSACHUSETTS CONSUMER PROTECTION ACT, MASS. GEN. LAWS ANN. CH. 93A, §§ 1, ET SEQ.
(ON BEHALF OF PLAINTIFFS JESSICA LEE ALLEN AND MINOR STUDENT C.A., JENNAANN BERRY AND MINOR STUDENT G.B., AND EMPLOYEE JONATHAN NEWELL AND MINOR STUDENTS B.R.N. AND B.D.N., AND THE MASSACHUSETTS SUBCLASS)

1289. Massachusetts Plaintiffs Jessica Lee Allen and Minor Student C.A., JennaAnn Berry and Minor Student G.B., and Employee Jonathan Newell and Minor Students B.R.N. and B.D.N. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1290. Plaintiffs, Massachusetts Subclass members, and Defendants are "persons" as meant by Mass. Gen. Laws. Ann. ch. 93A, § 1(a).

1291. Defendants operate in "trade or commerce" as meant by Mass. Gen. Laws Ann. ch. 93A, § 1(b).

1292. Plaintiffs sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3) on July 11, 2025.

1293. Defendants advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts as defined by Mass. Gen. Laws Ann. ch. 93A, § 1(b).

1294. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Massachusetts Subclass members' PII, 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, and adequately improve security and privacy

measures after previous cybersecurity incidents, 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 Massachusetts Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and their implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, §2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Massachusetts Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Massachusetts Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and their implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Massachusetts Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Massachusetts Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and their implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

1295. Defendants' acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that

Defendants alone held the true facts about their inadequate security for PII, which Plaintiffs and the Massachusetts Subclass members could not have independently discovered. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1296. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

1297. Defendants intended to mislead Plaintiffs and Massachusetts Subclass members and induce them to rely on their misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1298. Defendants acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act and recklessly disregarded Plaintiffs and Massachusetts Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1299. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and Massachusetts Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants

as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1300. Plaintiffs and Massachusetts Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, restitution; injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XLII - MICHIGAN IDENTITY THEFT PROTECTION ACT, MICH. COMP. LAWS ANN. §§ 445.72, ET SEQ.
(ON BEHALF OF PLAINTIFFS RUSHDA AFZAL AND MINOR STUDENTS Z.W., A.M.W., AND A.N.W, RATIB HABBAL AND MINOR STUDENT L.H., AND TRISHA NADEAU AND MINOR STUDENTS G.O.E. AND J.C.E., AND THE MICHIGAN SUBCLASS)

1301. Michigan Plaintiffs Rushda Afzal and Minor Students Z.W., A.M.W., and A.N.W, Ratib Habbal and Minor Student L.H., and Trisha Nadeau and Minor Students G.O.E. and J.C.E. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1302. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

1303. Plaintiffs' and Michigan Subclass members' PII includes Personal Information as covered under Mich. Comp. Laws Ann. § 445.72(1).

1304. Pursuant to Mich. Comp. Laws Ann. § 445.72(1), Defendants were required to accurately notify Plaintiffs and Michigan Subclass members of the Data Breach without unreasonable delay.

1305. Because Defendants discovered and had notice of a security breach in which unauthorized persons accessed or acquired unencrypted and unredacted Personal Information, it was obligated to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

1306. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Mich. Comp. Laws Ann. § 445.72(4).

1307. As a direct and proximate result of Defendants' violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiffs and Michigan Subclass members suffered damages, as described above.

1308. Plaintiffs and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT XLIII - MICHIGAN CONSUMER PROTECTION ACT, MICH. COMP. LAWS ANN. §§ 445.903, ET SEQ. (ON BEHALF OF PLAINTIFFS RUSHDA AFZAL AND MINOR STUDENTS Z.W., A.M.W., AND A.N.W, AND RATIB HABBAL AND MINOR STUDENT L.H., TRISHA NADEAU AND MINOR STUDENTS G.O.E. AND J.C.E., AND THE MICHIGAN SUBCLASS)

1309. Michigan Plaintiffs Rushda Afzal and Minor Students Z.W., A.M.W., and A.N.W and Ratib Habbal, and Minor Student L.H. and Trisha Nadeau and Minor Students G.O.E. and J.C.E. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1310. Plaintiffs, Michigan Subclass members, and Defendants are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

1311. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

1312. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

(b) Representing that their goods and services are of a particular standard or quality if they are of another, in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

(c) Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

(d) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

1313. Defendants' unfair, unconscionable, and deceptive practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Michigan Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Michigan Subclass members' PII,

including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Michigan Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Michigan Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1314. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1315. Defendants intended to mislead Plaintiffs and Michigan Subclass members and induce them to rely on their misrepresentations and omissions.

1316. Defendants acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act and recklessly disregarded Plaintiffs' and Michigan Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and

outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1317. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive practices, Plaintiffs and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1318. Plaintiffs and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or statutory damages in the amount of $250 for each Michigan Subclass member, restitution, injunctive relief, and any other relief that is just and proper.

COUNT XLIV – MINNESOTA CONSUMER FRAUD ACT, MINN. STAT. §§ 325F.68, ET SEQ. AND MINN. STAT. §§ 8.31, ET SEQ. (ON BEHALF OF PLAINTIFFS AMY HAUSER AND MINOR STUDENT J.H. AND THE MINNESOTA SUBCLASS)

1319. Minnesota Plaintiffs Amy Hauser and Minor Student J.H. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1320. Plaintiffs, Minnesota Subclass members, and Defendants are "persons" as defined by Minn. Stat. § 325F.68(3).

1321. Defendants' goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

1322. Defendants engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

1323. Defendants engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise in violation of Minn. Stat. § 325F.69(1), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Minnesota Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Minnesota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Minnesota Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Minnesota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Minnesota Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and

privacy of Plaintiffs' and Minnesota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1324. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1325. Defendants intended to mislead Plaintiffs and Minnesota Subclass members and induce them to rely on their misrepresentations and omissions.

1326. Defendants' fraudulent, misleading, and deceptive practices affected the public interest, including Minnesotans affected by the Data Breach.

1327. As a direct and proximate result of Defendants' fraudulent, misleading, and deceptive practices, Plaintiffs and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1328. Plaintiffs and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT XLV – MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,

MINN. STAT. §§ 325D.43, ET SEQ.

(ON BEHALF OF PLAINTIFFS AMY HAUSER AND MINOR STUDENT J.H. AND THE MINNESOTA SUBCLASS)

1329. Minnesota Plaintiffs Amy Hauser and Minor Student J.H. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1330. By engaging in deceptive trade practices in the course of their business and vocation directly or indirectly affecting the people of Minnesota, Defendants violated Minn. Stat. § 325D.44, including the following provisions:

(a) Representing that their goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

(b) Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

(c) Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

(d) Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

1331. Defendants' deceptive practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Minnesota Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Minnesota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Minnesota Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Minnesota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Minnesota Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Minnesota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1332. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1333. Defendants intended to mislead Plaintiffs and Minnesota Subclass members and induce them to rely on their misrepresentations and omissions.

1334. Had Defendants disclosed to Plaintiffs and Minnesota Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and class members' PII as part of the services

Defendants provided and for which Plaintiffs and Minnesota Subclass members paid without advising Plaintiffs and Minnesota Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Minnesota Subclass members' PII. Accordingly, Plaintiffs and the Minnesota Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1335. Defendants acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act and recklessly disregarded Plaintiffs' and Minnesota Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiffs and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1336. Plaintiffs and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

COUNT XLVI – MISSISSIPPI CONSUMER PROTECTION ACT, MISS. CODE §§ 75-24-1, ET SEQ.

(ON BEHALF OF PLAINTIFFS KATHEY HENRY AND MINOR STUDENTS T.M.H. AND T.T.H. AND THE MISSISSIPPI SUBCLASS)

1337. Mississippi Plaintiffs Kathey Henry and Minor Students T.M.H. And T.T.H. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1338. Defendants are "persons" as defined by Miss. Code § 75-24-3.

1339. Defendants advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

1340. Defendants engaged in unfair and deceptive trade acts or practices, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Mississippi Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Mississippi Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Mississippi Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Mississippi Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Mississippi Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Mississippi Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1341. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

(a) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

(c) Advertising goods or services with intent not to sell them as advertised.

1342. Defendants intended to mislead Plaintiffs and Mississippi Subclass members and induce them to rely on their misrepresentations and omissions.

1343. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1344. Had Defendants disclosed to Plaintiffs and Mississippi Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have been continued in business and would have been forced to adopt

reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Mississippi Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Mississippi Subclass members paid without advising Plaintiffs and Mississippi Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Mississippi Subclass members' PII. Accordingly, Plaintiffs and the Mississippi Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1345. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensiveness of the PII in their possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Mississippi Subclass—and Defendants because consumers cannot fully protect their interests regarding their data and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems and their prior data breaches while purposefully withholding material facts from Plaintiffs and the Mississippi Subclass that contradicted these representations.

1346. Defendants acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act and recklessly disregarded Plaintiff and Mississippi Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security

measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1347. As a direct and proximate result of Defendants' unfair and deceptive acts or practices and Plaintiffs' and Mississippi Subclass members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiffs and Mississippi Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1348. Defendants' violations present a continuing risk to Plaintiffs and Mississippi Subclass members as well as to the general public.

1349. Plaintiffs and Mississippi Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

COUNT XLVII – MISSOURI MERCHANDISING PRACTICES ACT, MO. REV. STAT. §§ 407.010, ET SEQ.
(ON BEHALF OF PLAINTIFFS KRISTI KINGERY-ISLAS, TORRIE MAYFEILD AND MINOR STUDENT A.M., FORMER STUDENT JACOB ISLAS, AND THE MISSOURI SUBCLASS)

1350. Missouri Plaintiffs Kristi Kingery-Islas, Torrie Mayfeild and Minor Student A.M., and Former Student Jacob Islas ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1351. Defendants are "persons" as defined by Mo. Rev. Stat. § 407.010(5).

1352. Defendants advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

1353. Plaintiffs and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

1354. Defendants engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce in violation of Mo. Rev. Stat. § 407.020(1), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Missouri Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Missouri Subclass members' PII, including

duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Missouri Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Missouri Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Missouri Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy Plaintiffs' and Missouri Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1355. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1356. Defendants intended to mislead Plaintiffs and Missouri Subclass members and induce them to rely on their misrepresentations and omissions.

1357. Defendants acted intentionally, knowingly, and maliciously to violate Missouri's Merchandising Practices Act and recklessly disregarded Plaintiffs' and Missouri Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and

outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1358. As a direct and proximate result of Defendants' unlawful, unfair, and deceptive acts and practices, Plaintiffs and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1359. Plaintiffs and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

COUNT XLVIII – COMPUTER SECURITY BREACH LAW, MONT. CODE ANN. §§ 30-14-1704(1), ET SEQ. (ON BEHALF OF PLAINTIFFS KATHLEEN HOLM AND MINOR STUDENTS P.P. AND R.P AND THE MONTANA SUBCLASS)

1360. Montana Plaintiffs Kathleen Holm and Minor Students P.P. and R.P ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1361. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Mont. Code Ann. § 30-14-1704(4)(b). Defendants also maintain computerized data that includes Personal Information not owned by Defendants. Defendants are thus subject to Mont. Code Ann. § 30-14-1704(1) and (2).

1362. Plaintiffs' and Montana Subclass members' PII includes Personal Information covered by Mont. Code Ann. § 30-14-1704(4)(b).

1363. Pursuant to Mont. Code Ann. § 30-14-1704(2), Defendants were required to provide Plaintiffs and Montana Subclass members accurate notice of the Data Breach without unreasonable delay.

1364. Under Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30- 14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

1365. As a direct and proximate result of Defendants' violations of Mont. Code Ann. § 30- 14-1704(1) and (2), Plaintiffs and Montana Subclass members suffered damages, as described above.

1366. Plaintiffs and Montana Subclass members seek relief under Mont. Code Ann. § 30- 14-133, including actual damages and injunctive relief.

COUNT XLIX – MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, M.C.A. §§ 30-14-101, ET SEQ. (ON BEHALF OF PLAINTIFFS KATHLEEN HOLM AND MINOR STUDENTS P.P. AND R.P AND THE MONTANA SUBCLASS)

1367. Montana Plaintiffs Kathleen Holm and Minor Students P.P. and R.P ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1368. Defendants are "persons" as defined by MCA § 30-14-102(6).

1369. Plaintiffs and Montana Subclass members are "consumers" as defined by MCA§ 30- 14-102(1).

1370. Defendants advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana as defined by MCA § 30-14-102(8).

1371. Defendants engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Montana Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Montana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Montana Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Montana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Montana Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Montana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1372. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1373. Had Defendants disclosed to Plaintiffs and Montana Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Montana Subclass members' Personal Information as part of the services Defendants provided and for which Plaintiffs and Montana Subclass members paid without advising Plaintiffs and Montana Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Montana Subclass members' Personal Information. Accordingly, Plaintiff and the Montana Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1374. Defendants' acts described above are not only unfair and offend public policy—they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

1375. Defendants acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act and recklessly disregarded Plaintiffs' and Montana Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1376. As a direct and proximate result of Defendants' unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiffs and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1377. Plaintiffs and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

COUNT L – NOTICE OF SECURITY BREACH,
N.H. REV. STAT. ANN. §§ 359-C:20(I)(A), ET SEQ.
(ON BEHALF OF PLAINTIFFS SERENE BAVIS AND MINOR STUDENT S.W. AND THE NEW HAMPSHIRE SUBCLASS)

1378. New Hampshire Plaintiffs Serene Bavis and Minor Student S.W. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1379. Defendants are businesses that own or license computerized data that includes Personal Information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1380. Plaintiffs' and New Hampshire Subclass members' PII includes Personal Information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1381. Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Defendants were required to accurately notify Plaintiffs and New Hampshire Subclass members of the Data Breach as soon as possible.

1382. Because Defendants were aware of a security breach in which misuse of Personal Information has occurred or is reasonably likely to occur, Defendants were obligated to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359- C:20(I)(a).

1383. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1384. As a direct and proximate result of Defendants' violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiffs and New Hampshire Subclass members suffered damages, as described above.

1385. Plaintiffs and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

COUNT LI – NEW HAMPSHIRE CONSUMER PROTECTION ACT, N.H.R.S.A. §§ 358-A, ET SEQ.
(ON BEHALF OF PLAINTIFFS SERENE BAVIS AND MINOR STUDENT S.W., KELSEY GAURON AND R.M.M., AND THE NEW HAMPSHIRE SUBCLASS)

1386. New Hampshire Plaintiffs Serene Bavis and Minor Student S.W., and Kelsey Gauron and R.M.M. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1387. Defendants are "persons" under the New Hampshire Consumer Protection Act.

1388. Defendants advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire as defined by N.H.R.S.A. § 358-A:1.

1389. Defendants engaged in unfair and deceptive acts or practices in the ordinary conduct of their trade or business in violation of N.H.R.S.A. § 358-A:2, including:

(a) Representing that their goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V;

(b) Representing that their goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and

(c) Advertising their goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.

1390. Defendants' unfair and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New Hampshire Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 New Hampshire Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and New Hampshire Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Hampshire Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and New Hampshire Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Hampshire Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1391. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1392. Defendants acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiffs' and New Hampshire Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1393. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity;

time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1394. Plaintiffs and New Hampshire Subclass members seek all monetary and non- monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

COUNT LII – NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT,
N.J. STAT. ANN. §§ 56:8-163, ET SEQ.
(ON BEHALF OF PLAINTIFFS SAKINAH ARDINE KNOTT AND MINOR STUDENTS M.M.W., D.J.P., AND I.M.W., MELISSA GIFFORD AND MINOR STUDENTS J.R.M, C.A.M. AND J.S.M., AND THE NEW JERSEY SUBCLASS)

1395. New Jersey Plaintiffs Sakinah Ardine Knott and Minor Students M.M.W., D.J.P., and I.M.W., and Melissa Gifford and Minor Students J.R.M, C.A.M., and J.S.M. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1396. Defendants are businesses that conduct business in New Jersey under N.J. Stat. Ann. § 56:8-163(a).

1397. Plaintiffs' and New Jersey Subclass members' PII includes Personal Information covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

1398. Under N.J. Stat. Ann. § 56:8-163(a), "[a]ny business that conducts business in New Jersey . . . shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

1399. Because Defendants discovered a breach of their security system in which Personal Information was or is reasonably believed to have been acquired by an unauthorized person, and the Personal Information was not secured, Defendants were obligated to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

1400. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.J. Stat. Ann. § 56:8-163(a).

1401. As a direct and proximate result of Defendants' violations of N.J. Stat. Ann. § 56:8- 163(a), Plaintiffs and New Jersey Subclass members suffered the damages described above.

1402. Plaintiffs and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8- 19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT LIII – NEW JERSEY CONSUMER FRAUD ACT, N.J. STAT. ANN. §§ 56:8-1, ET SEQ. (ON BEHALF OF PLAINTIFFS SAKINAH ARDINE KNOTT AND MINOR STUDENTS M.M.W., D.J.P., AND I.M.W., MELISSA GIFFORD AND MINOR CHILDREN J.R.M, C.A.M. AND J.S.M., AND THE NEW JERSEY SUBCLASS)

1403. New Jersey Plaintiffs Sakinah Ardine Knott and Minor Children M.M.W., D.J.P., and I.M.W., and Melissa Gifford and Minor Children J.R.M, C.A.M., and J.S.M ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1404. Defendants are "persons" as defined by N.J. Stat. Ann. § 56:8-1(d).

1405. Defendants sell "merchandise" as defined by N.J. Stat. Ann. §§ 56:8-1(c) & (e).

1406. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, and misrepresentation as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on that concealment, omission, or fact in connection with the sale or advertisement of any merchandise.

1407. Defendants' unconscionable and deceptive practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New Jersey Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 New Jersey Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and New Jersey Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Jersey Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and New Jersey Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Jersey Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1408. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1409. Defendants intended to mislead Plaintiffs and New Jersey Subclass members and induce them to rely on their misrepresentations and omissions.

1410. Defendants acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and New Jersey Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1411. As a direct and proximate result of Defendants' unconscionable and deceptive practices, Plaintiffs and New Jersey Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1412. Plaintiffs and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT LIV – NEW MEXICO UNFAIR PRACTICES ACT, N.M. STAT. ANN. §§ 57-12-2, ET SEQ.
(ON BEHALF OF PLAINTIFFS TEACHER KAITLYN GILLIS AND MINOR STUDENT W.C.G. AND THE NEW MEXICO SUBCLASS)

1413. New Mexico Plaintiffs Teacher Kaitlyn Gillis and Minor Student W.C.G. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1414. Defendants are "persons" as meant by N.M. Stat. Ann. § 57-12-2.

1415. Defendants were engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

1416. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, et seq., prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

1417. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of their trade or commerce, including the following:

(a) Knowingly representing that their goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5);

(b) Knowingly representing that their goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7);

(c) Knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14);

(d) Taking advantage of the lack of knowledge, experience, or capacity of their consumers to a grossly unfair degree to Plaintiffs' and New Mexico Subclass members' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and

(e) Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiffs and New Mexico Subclass members and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

1418. Defendants' unfair, deceptive, and unconscionable acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New Mexico Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 New Mexico Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and New Mexico Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Mexico Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and New Mexico Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Mexico Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4.

1419. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1420. Defendants intended to mislead Plaintiffs and New Mexico Subclass members and induce them to rely on their misrepresentations and omissions.

1421. Defendants acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act and recklessly disregarded Plaintiff and New Mexico Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1422. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable trade practices, Plaintiffs and New Mexico Subclass members have

suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1423. Plaintiffs and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

COUNT LV – NEW YORK GENERAL BUSINESS LAW,
N.Y. GEN. BUS. LAW §§ 349, ET SEQ.
(ON BEHALF OF PLAINTIFFS JENNIFER CECILIA HARRELL AND MINOR STUDENT J.E.H., PATRICK BOWER AND MINOR STUDENT J.B., AND THE NEW YORK SUBCLASS)

1424. New York Plaintiffs Jennifer Cecelia Harrell and Minor Student J.H., Patrick Bower and Minor Student J.B. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1425. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 New York Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and New York Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and New York Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1426. Plaintiffs and New York Subclass members were deceived in New York. They also transacted with Defendants in New York by using Defendants products in New York.

1427. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1428. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law and recklessly disregarded Plaintiffs' and New York Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1429. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiffs and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1430. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach. Defendants' above-described deceptive and unlawful practices and acts caused substantial injury to Plaintiffs and New York Subclass members that they could not reasonably avoid.

1431. Plaintiffs and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

COUNT LVI – NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. GEN. STAT. §§ 75-60, ET SEQ.
(ON BEHALF OF PLAINTIFFS EMPLOYEE KIMBERLY GREER, TEACHER JUSTINE SHAMEY, KRISTIN ECKART AND MINOR STUDENTS J.E. AND T.E., JESSICA PATRICK TAYLOR AND MINOR STUDENTS J.O.P. AND N.O.T., FORMER STUDENT AYEDON BAUDER, AND TEACHER CHRISTOPHER JOSEPH WAGONER, AND THE NORTH CAROLINA SUBCLASS)

1432. North Carolina Plaintiffs Employee Kimberly Greer, Teacher Justine Shamey, Kristin Eckart and Minor Students J.E. and T.E., Jessica Patrick Taylor and Minor Students J.O.P. and N.O.T., Former Student Ayedon Bauder, and Teacher Christopher Joseph Wagoner ("Plaintiffs" for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1433. Defendants are businesses that own or license computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

1434. Plaintiffs and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

1435. Plaintiffs' and North Carolina Subclass members' PII includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

1436. Pursuant to N.C. Gen. Stat. § 75-65, Defendants were required to accurately notify Plaintiffs and North Carolina Subclass members of the Data Breach without unreasonable delay.

1437. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.C. Gen. Stat. § 75-65.

1438. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

1439. Because Defendnants discovered and had notice of a security breach in which unauthorized persons accessed or acquired unencrypted and unredacted Personal Information, Defendants were obligated to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

1440. As a direct and proximate result of Defendants' violations of N.C. Gen. Stat. § 75-65, Plaintiffs and North Carolina Subclass members suffered damages, as described above.

1441. Plaintiffs and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT LVII – NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. GEN. STAT. ANN. §§ 75-1.1, ET SEQ.
(ON BEHALF OF PLAINTIFFS EMPLOYEE KIMBERLY GREER, TEACHER JUSTINE SHAMEY, KRISTIN ECKART AND MINOR STUDENTS J.E. AND T.E., JESSICA PATRICK TAYLOR AND MINOR STUDENTS J.O.P. AND N.O.T., FORMER STUDENT AYEDON BAUDER, AND TEACHER CHRISTOPHER JOSEPH WAGONER, AND THE NORTH CAROLINA SUBCLASS)

1442. North Carolina Plaintiffs Employee Kimberly Greer, Teacher Justine Shamey, Kristin Eckart and Minor Students J.E. and T.E., Jessica Patrick Taylor and Minor Students J.O.P. and N.O.T., Former Student Ayedon Bauder, and Teacher Christopher Joseph Wagoner ("Plaintiffs" for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1443. Defendants advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

1444. Defendants engaged in unfair and deceptive acts and practices in or affecting commerce in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and North Carolina Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 North Carolina Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and North Carolina Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and North Carolina Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and North Carolina Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and North Carolina Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1445. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1446. Defendants intended to mislead Plaintiffs and North Carolina Subclass members and induce them to rely on their misrepresentations and omissions.

1447. Had Defendants disclosed to Plaintiffs and North Carolina Subclass members that their data systems were not secure and were thus vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and North Carolina Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and North Carolina Subclass members paid without advising Plaintiffs and North Carolina Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and North Carolina Subclass members' PII. Accordingly, Plaintiffs and the North Carolina Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1448. Defendants acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act and recklessly disregarded Plaintiffs' and North Carolina Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1449. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid

less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1450. Defendants' conduct as alleged herein was continuous such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

1451. Plaintiffs and North Carolina Subclass members seek all monetary and non- monetary relief allowed by law, including actual damages, treble damages, restitution, and attorneys' fees and costs.

COUNT LVIII - NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION, N.D. CENT. CODE §§ 51-30-02, ET SEQ. (ON BEHALF OF PLAINTIFFS MARIAH JENE MARTYN AND MINOR STUDENT L.M.A. AND THE NORTH DAKOTA SUBCLASS)

1452. North Dakota Plaintiffs Mariah Jene Martyn and Minor Student L.M.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1453. Defendants are businesses that own or license computerized data that includes Personal Information as defined by N.D. Cent. Code § 51-30-01(4). Defendants also maintain computerized data that includes Personal Information not owned by Defendants. Accordingly, they are subject to N.D. Cent. Code §§ 51-30-02 and 03.

1454. Plaintiffs' and North Dakota Subclass members' PII includes Personal Information covered by N.D. Cent. Code § 51-30-01(4).

1455. Under N.D. Cent. Code § 51-30-03, Defendants must give immediate notice of a breach of security of a data system to owners of Personal Information not owned by Defendants, including Plaintiffs and North Dakota Subclass members.

1456. Under N.D. Cent. Code § 51-30-02, if Defendants discovers or receives notice of a security breach that may have compromised Personal Information Defendants own or license, it must—in the most expedient time possible and without unreasonable delay—accurately notify Plaintiffs and North Dakota Subclass members.

1457. Because Defendants were aware of a security breach, Defendants were obligated to disclose the data breach as mandated by N.D. Cent. Code §§ 51-30-02 and 51-30-03.

1458. Under N.D. Cent. Code § 51-30-07, violations of N.D. Cent. Code §§ 51-30- 02 and 51-30-03 are unlawful sales or advertising practices that violate chapter 51-15 of the North Dakota Century Code.

1459. As a direct and proximate result of Defendants' violations of N.D. Cent. Code §§ 51- 30-02 and 51-30-03, Plaintiffs and North Dakota Subclass members suffered damages, as described above.

1460. Plaintiffs and North Dakota Subclass members seek relief under N.D. Cent. Code §§ 51-15-01 et seq., including actual damages and injunctive relief.

COUNT LIX - NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT, N.D. CENT. CODE §§ 51-15-01, ET SEQ.
(ON BEHALF OF PLAINTIFFS MARIAH JENE MARTYN AND MINOR STUDENT L.M.A. AND THE NORTH DAKOTA SUBCLASS)

1461. North Dakota Plaintiffs Mariah Jene Martyn and Minor Student L.M.A. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1462. Plaintiffs, North Dakota Subclass members, and Defendants are "persons" as defined by N.D. Cent. Code § 51-15-01(4). 630. Defendants sell and advertise "merchandise" as defined by N.D. Cent. Code § 51- 15-01(3) and (5).

1463. Defendants advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota. 632.Defendants engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise in violation of N.D. Cent. Code § 51-15-01, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and North Dakota Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 North Dakota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and North Dakota Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and North Dakota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and North Dakota Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and North Dakota Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1464. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII

1465. Defendants' above-described acts and practices caused substantial injury to Plaintiffs and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1466. Defendants intended to mislead Plaintiffs and North Dakota Subclass members and induce them to rely on their misrepresentations and omissions.

1467. Defendants acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law and recklessly disregarded Plaintiffs' and North Dakota Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1468. As a direct and proximate result of Defendants' deceptive, unconscionable, and substantially injurious practices, Plaintiffs and North Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, including loss of the

benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1469. Plaintiffs and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

COUNT LX – OHIO CONSUMER SALES PRACTICES ACT, OHIO REV. CODE §§ 1345.01, ET SEQ. (ON BEHALF OF PLAINTIFFS ANDREW COOK AND MINOR STUDENTS A.C. AND C.C., AND FORMER STUDENT EVAN GRAMELSPACHER, AND THE OHIO SUBCLASS)

1470. Ohio Plaintiffs Andrew Cook and Minor Students A.C. and C.C. and Former Student Evan Gramelspacher ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1471. Plaintiffs, Ohio Subclass members, and Defendants are "persons" as defined by Ohio Rev. Code § 1345.01(B).

1472. Defendants are "suppliers" engaged in "consumer transactions" as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

1473. Defendants advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1474. Defendants engaged in unfair and deceptive acts and practices in connection with a consumer transaction in violation of Ohio Rev. Code §§ 1345.02, including:

(a) representing that their goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

(b) representing that their goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

1475. Defendants engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

(a) knowingly taking advantage of Plaintiffs' and Ohio Subclass members' inability to reasonably protect their interests because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

(b) requiring Plaintiffs and Ohio Subclass members to enter into a consumer transaction on terms that Defendants knew were substantially one-sided in favor of itself (Ohio Rev. Code Ann. § 1345.03(B)(5)).

1476. Defendants' unfair, deceptive, and unconscionable acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Ohio Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Ohio Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Ohio Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Ohio Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1477. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1478. Defendants intended to mislead Plaintiffs and Ohio Subclass members and induce them to rely on their misrepresentations and omissions.

1479. Defendants acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act and recklessly disregarded Plaintiffs' and Ohio Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1480. Defendants' unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

1481. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable acts and practices, Plaintiffs and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1482. Plaintiffs and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

COUNT LXI – OHIO DECEPTIVE TRADE PRACTICES ACT, OHIO REV. CODE §§ 4165.01, ET SEQ.
(ON BEHALF OF PLAINTIFFS ANDREW COOK AND MINOR STUDENTS A.C. AND C.C., AND FORMER STUDENT EVAN GRAMELSPACHER, AND THE OHIO SUBCLASS)

1483. Ohio Plaintiffs Andrew Cook and Minor Students A.C. and C.C. and Former Student Evan Gramelspacher ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1484. Defendants, Plaintiffs, and Ohio Subclass members are "persons" as defined by Ohio Rev. Code § 4165.01(D).

1485. Defendants advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1486. Defendants engaged in deceptive trade practices in the course of their business and vocation in violation of Ohio Rev. Code § 4165.02, including:

(a) Representing that their goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

(b) Representing that their goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

(c) Advertising their goods and services with intent not to sell them as advertised, in violation of Ohio Rev. Code § 4165.02(A)(11).

1487. Defendants' deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Ohio Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 Ohio Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Ohio Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Ohio Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1488. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1489. Defendants intended to mislead Plaintiffs and Ohio Subclass members and induce them to rely on their misrepresentations and omissions.

1490. Defendants acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1491. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiffs and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not

have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1492. Plaintiffs and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, restitution, attorneys' fees, and any other relief that is just and proper.

COUNT LXII - OKLAHOMA CONSUMER PROTECTION ACT, OKLA. STAT. TIT. 15, §§ 751, ET SEQ.
(ON BEHALF OF PLAINTIFF TEACHER PAUL THOMPSON AND THE OKLAHOMA SUBCLASS)

1493. Oklahoma Plaintiff Teacher Paul Thompson ("Plaintiff," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1494. Defendants are "persons" as meant by Okla. Stat. tit. 15, § 752(1).

1495. Defendants' advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

1496. Defendants, in the course of their business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

(a) Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of their consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);

(b) Representing, knowingly or with reason to know, that the subjects of their consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);

(c) Advertising, knowingly or with reason to know, the subjects of their consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);

(d) Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

(e) Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

1497. Defendants' unlawful practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Oklahoma Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Plaintiff's and Oklahoma Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that they would protect the privacy and confidentiality Plaintiff's and Oklahoma Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Oklahoma Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Oklahoma Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Oklahoma Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1498. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1499. Defendants intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on their misrepresentations and omissions.

1500. Had Defendants disclosed to Plaintiff and Oklahoma Subclass members that their data systems were not secure and, thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Oklahoma Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Oklahoma Subclass members paid without advising Plaintiff and Oklahoma Subclass members that Defendants' data security practices were insufficient to maintain the safety and

confidentiality of Plaintiff's and Oklahoma Subclass members' PII. Accordingly, Plaintiffs and the Oklahoma Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1501. Defendants' above-described unlawful practices and acts were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

1502. Defendants acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act and recklessly disregarded Plaintiff's and Oklahoma Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiff's and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1503. As a direct and proximate result of Defendants' unlawful practices, Plaintiff and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1504. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

COUNT LXIII – OREGON CONSUMER IDENTITY THEFT PROTECTION ACT,

OR. REV. STAT. §§ 646A.604(1), ET SEQ.

(ON BEHALF OF PLAINTIFFS CARA LEWIS AND MINOR STUDENTS A.L. AND M.L. AND THE OREGON SUBCLASS)

1505. Oregon Plaintiffs Cara Lewis and Minor Students A.L. and M.L. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1506. Defendants are businesses that maintain records which contain Personal Information, within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiffs and Oregon Subclass members.

1507. Plaintiffs' and Oregon Subclass members' PII includes Personal Information as covered under Or. Rev. Stat. § 646A.604(1).

1508. Under Or. Rev. Stat. § 646A.622(1), a business "that maintain records which contain Personal Information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

1509. Defendants violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiffs' and Oregon Subclass members' PII.

1510. Defendants are businesses that own, maintain, or otherwise possess data that includes consumers' Personal Information as defined by Or. Rev. Stat. § 646A.604(1).

1511. Under Or. Rev. Stat. § 646A.604(1), if Defendants becomes aware of a breach of their data security system, it must accurately notify—in the most expeditious

time possible and without unreasonable delay—Plaintiff and Oregon Subclass members.

1512. Because Defendants discovered a breach of their security system, it was obligated to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

1513. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Or. Rev. Stat. § 646A.604(1).

1514. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

1515. As a direct and proximate result of Defendants' violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiffs and Oregon Subclass members suffered damages, as described above.

1516. Plaintiffs and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

COUNT LXIV – OREGON UNLAWFUL TRADE PRACTICES ACT, OR. REV. STAT. §§ 646.608, ET SEQ.
(ON BEHALF OF PLAINTIFFS CARA LEWIS AND MINOR STUDENTS A.L. AND M.L. AND THE OREGON SUBCLASS)

1517. Oregon Plaintiffs Cara Lewis and Minor Students A.L. and M.L. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1518. Defendants are "persons" as defined by Or. Rev. Stat. § 646.605(4).

1519. Defendants engaged in the sale of "goods and services" as defined by Or. Rev. Stat. § 646.605(6)(a).

1520. Defendants sold "goods or services" as defined by Or. Rev. Stat. § 646.605(6)(a).

1521. Defendants advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

1522. Defendants engaged in unlawful practices in the course of their business and occupation, in violation of Or. Rev. Stat. § 646.608, including the following:

(a) Representing that their goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

(b) Representing that their goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

(c) Advertising their goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

(d) Concurrent with tender or delivery of their goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

1523. Defendants' unlawful practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Oregon Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Oregon Subclass members' PII including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq., which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Oregon Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Oregon Subclass members' PII.

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.

1524. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1525. Defendants intended to mislead Plaintiffs and Oregon Subclass members and induce them to rely on their misrepresentations and omissions.

1526. Had Defendants disclosed to Plaintiffs and Oregon Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Oregon Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Oregon Subclass members paid without advising Plaintiffs and Oregon Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of

Plaintiffs' and Oregon Subclass members' PII. Accordingly, Plaintiffs and the Oregon Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1527. Defendants acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act and recklessly disregarded Plaintiffs' and Oregon Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1528. As a direct and proximate result of Defendants' unlawful practices, Plaintiffs and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1529. Plaintiffs and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, restitution, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

COUNT LXV – PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,
73 PA. CONS. STAT. §§ 201-2 & 201-3, ET SEQ.
(ON BEHALF OF PLAINTIFFS JOHN TRZCINSKI AND MINOR STUDENTS E.T. AND S.T. AND THE PENNSYLVANIA SUBCLASS)

1530. Pennsylvania Plaintiffs John Trzcinski and Minor Students E.T. and S.T. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1531. Defendants are "persons" as defined by 73 Pa. Cons. Stat. § 201-2(2).

1532. Plaintiffs and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce" as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes, directly or indirectly.

1533. Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of their trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

(a) Representing that their goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

(b) Representing that their goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

(c) Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

1534. Defendants' unfair or deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Pennsylvania Subclass members' PII, 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, and adequately improve security and privacy

measures after previous cybersecurity incidents, 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 Pennsylvania Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Pennsylvania Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Pennsylvania Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Pennsylvania Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Pennsylvania Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1535. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1536. Defendants intended to mislead Plaintiffs and Pennsylvania Subclass members and induce them to rely on their misrepresentations and omissions.

1537. Had Defendants disclosed to Plaintiffs and Pennsylvania Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants

received, maintained, and compiled Plaintiffs' and Pennsylvania Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Pennsylvania Subclass members paid without advising Plaintiffs and Pennsylvania Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Pennsylvania Subclass members' PII. Accordingly, Plaintiffs and the Pennsylvania Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1538. Defendants acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law and recklessly disregarded Plaintiffs' and Pennsylvania Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1539. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs' and Pennsylvania Subclass members' reliance on them, Plaintiffs and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and

replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1540. Plaintiffs and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT LXVI – RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT, R.I. GEN. LAWS §§ 6-13.1, ET SEQ.

(ON BEHALF OF PLAINTIFF TEACHER DENISE CHAMPNEY AND THE RHODE ISLAND SUBCLASS)

1541. Rhode Island Plaintiff Teacher Denise Champney ("Plaintiff," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1542. Plaintiff, Rhode Island Subclass members, and Defendants are "persons" as defined by R.I. Gen. Laws § 6-13.1-1(3).

1543. Plaintiff and Rhode Island Subclass members purchased goods and services from Defendants, directly or indirectly, for personal, family, or household purposes.

1544. Defendants advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island as defined by R.I. Gen. Laws § 6-13.1-1(5).

1545. Defendants engaged in unfair and deceptive acts and practices in violation of R.I. Gen. Laws § 6-13.1-2, including:

(a) Representing that their goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v));

(b) Representing that their goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii));

(c) Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix));

(d) Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii));

(e) Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and

(f) Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

1546. Defendants' unfair and deceptive acts include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Rhode Island Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Plaintiff's and Rhode Island Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality Plaintiff's and Rhode Island Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Rhode Island

Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Rhode Island Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Rhode Island Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

1547. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1548. Defendants intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on their misrepresentations and omissions.

1549. Defendants acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Rhode Island Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiff's and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1550. As a direct and proximate result of Defendants' unfair and deceptive acts, Plaintiff and Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they

would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

1551. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, restitution and other equitable relief, and attorneys' fees and costs.

COUNT LXVII – SOUTH CAROLINA DATA BREACH SECURITY ACT, S.C. CODE ANN. §§ 39-1-90, ET SEQ.
(ON BEHALF OF PLAINTIFFS NICOLE DRENNEN AND MINOR STUDENTS G.D. AND Q.D., SAMARIAH LOCKHART AND MINOR STUDENT P.M., KRYSTAL VARGHA, AND MINOR STUDENTS A.V., B.V., AND G.V., AND SHAWN FRIEDMAN AND MINOR STUDENT J.F. AND THE SOUTH CAROLINA SUBCLASS)

1552. South Carolina Plaintiffs Nicole Drennen and Minor Students G.D. and Q.D., Samariah Lockhart and Minor Student P.M., Krystal Vargha, and Minor Students A.V., B.V., and G.V., and Shawn Friedman and Minor Student J.F. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1553. Defendants are businesses that own or license computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

1554. Plaintiffs' and South Carolina Subclass members' PII includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

1555. Under S.C. Code Ann. § 39-1-90(A), Defendants must—in the most expedient time possible and without unreasonable delay—accurately notify Plaintiffs and South Carolina Subclass members after discovery or notification of a breach of their data security system if PII that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm,

1556. Because Defendants discovered a breach of their data security system in which PII that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Defendants were obligated to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

1557. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated S.C. Code Ann. § 39-1-90(A).

1558. As a direct and proximate result of Defendants' violations of S.C. Code Ann. § 39-1- 90(A), Plaintiffs and South Carolina Subclass members suffered damages, as described above.

1559. Plaintiffs and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT LXVIII – SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT, S.C. CODE ANN. §§ 39-5-10, ET SEQ.
(ON BEHALF OF PLAINTIFFS NICOLE DRENNEN AND MINOR STUDENTS G.D. AND Q.D., SAMARIAH LOCKHART AND MINOR STUDENT P.M., KRYSTAL VARGHA, AND MINOR STUDENTS A.V., B.V., AND G.V., AND SHAWN FRIEDMAN AND MINOR STUDENT J.F. AND THE SOUTH CAROLINA SUBCLASS)

1560. South Carolina Plaintiffs Nicole Drennen and Minor Students G.D. and Q.D., Samariah Lockhart and Minor Student P.M., Krystal Vargha, and Minor Students

A.V., B.V., and G.V., and Shawn Friedman and Minor Student J.F. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1561. Defendants are "persons" as defined by S.C. Code Ann. § 39-5-10(a).

1562. South Carolina's Unfair Trade Practices Act ("UTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

1563. Defendants advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

1564. Defendants engaged in unfair and deceptive acts and practices, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and South Carolina Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 South Carolina Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and South Carolina Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and South Carolina Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and South Carolina Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and South Carolina Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1565. Defendants' acts and practices had, and continue to have, the tendency or capacity to deceive.

1566. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1567. Defendants intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on their misrepresentations and omissions.

1568. Had Defendants disclosed to Plaintiffs and Class Members that their data systems were not secure and, thus, vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and South Carolina Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and South Carolina Subclass members paid without advising Plaintiffs and South Carolina Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and South Carolina Subclass members' PII. Accordingly, Plaintiffs and the South Carolina Subclass members acted reasonably in relying on

Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1569. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiffs and the South Carolina Subclass—and Defendants because consumers are unable to fully protect their interests with regard to the PII in Defendants' possession, and place trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches while purposefully withholding material facts from Plaintiffs and the South Carolina Subclass that contradicted these representations.

1570. Defendants' business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Defendants' acts and practices offend established public policies that seek to protect consumers' PII and ensure that entities entrusted with PII use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45, and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, et seq.

1571. Defendants' failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Defendants' long history of inadequate data security and previous data breaches and the sensitivity and extensiveness of Personal Information in their possession.

1572. Defendants' unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Defendants engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including the many South Carolinians impacted by the Data Breach.

1573. Defendants' unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Defendants' policies and procedures, such as their security practices, create the potential for recurrence of the complained-of business acts and practices.

1574. Defendants' violations present a continuing risk to Plaintiffs and South Carolina Subclass members as well as to the general public.

1575. Defendants intended to mislead Plaintiffs and South Carolina Subclass members and induce them to rely on their misrepresentations and omissions.

1576. Defendants acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act and recklessly disregarded Plaintiffs and South Carolina Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct and would deter Defendants and others from committing similar conduct in the future.

1577. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiffs and South Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1578. Plaintiffs and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT LXIX - TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, TENN. CODE ANN. §§ 47-18-2107, ET SEQ. (ON BEHALF OF PLAINTIFFS AMY LANCASTER AND MINOR STUDENTS E.M.L., K.C.L., AND C.S.R.L.AND THE TENNESSEE SUBCLASS)

1579. Tennessee Plaintiffs Amy Lancaster and Minor Students E.M.L., K.C.L., and C.S.R.L. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1580. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

1581. Plaintiffs' and Tennessee Subclass members' PII includes Personal Information as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

1582. Defendants are required to accurately notify Plaintiff and Tennessee Subclass members after discovery or notification of a breach of their data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

1583. Because Defendants discovered a breach of their security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, Defendants were obligated to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

1584. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Tenn. Code Ann. § 47-18-2107(b).

1585. As a direct and proximate result of Defendants' violations of Tenn. Code Ann. § 47- 18-2107(b), Plaintiffs and Tennessee Subclass members suffered damages, as described above.

1586. Plaintiffs and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

COUNT LXX - TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, TENN. CODE ANN. §§ 47-18-2107, ET SEQ. (ON BEHALF OF PLAINTIFFS AMY LANCASTER AND MINOR STUDENTS E.M.L., K.C.L., AND C.S.R.L.AND THE TENNESSEE SUBCLASS)

1587. Tennessee Plaintiffs Amy Lancaster and Minor Students E.M.L., K.C.L., and C.S.R.L. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1588. Defendants are "persons" as defined by Tenn. Code § 47-18-103(13).

1589. Plaintiffs and Tennessee Subclass members are "consumers" as meant by Tenn. Code § 47-18-103(2).

1590. Defendants advertised and sold "goods" or "services" in "consumer transaction[s]" as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

1591. Defendants advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Defendants' acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

1592. Defendants' unfair and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Tennessee Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Tennessee Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Tennessee Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Tennessee Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Tennessee Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Tennessee Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1593. Defendants intended to mislead Plaintiffs and Tennessee Subclass members and induce them to rely on their misrepresentations and omissions.

1594. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

1595. Had Defendants disclosed to Plaintiffs and Tennessee Subclass members that their data systems were not secure and, thus, vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Tennessee Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Tennessee Subclass members paid without advising Plaintiffs and Tennessee Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of could not have continued. Accordingly, Plaintiffs and the Tennessee Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1596. Defendants had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the Personal Information in their possession. This duty arose because Plaintiffs and the Tennessee Subclass members

reposed trust and confidence in Defendants when they provided their PII to Defendants in exchange for Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Subclass, and Defendants because consumers are unable to fully protect their interests with regard to their data and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiffs and the Tennessee Subclass that contradicted these representations.

1597. Defendants' "unfair" acts and practices caused or were likely to cause substantial injury to consumers that was not reasonably avoidable by consumers themselves or outweighed by countervailing benefits to consumers or to competition.

1598. The injury to consumers was and is substantial because it was non-trivial, non- speculative, and involved a monetary injury and/or an unwarranted risk to the safety of consumers' PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers but also because it inflicted a significant amount of harm on each consumer.

1599. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security, Defendants

created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1600. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

1601. By misrepresenting and omitting material facts about their data security and failing to comply with their common law and statutory duties pertaining to data security (including their duties under the FTC Act), Defendants violated the following provisions of Tenn. Code § 47-18-104(b): a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; c. Advertising goods or services with intent not to sell them as advertised; d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

1602. Defendants acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act and recklessly disregarded Plaintiffs' and Tennessee Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1603. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiffs and Tennessee Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses

from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1604. Defendants' violations present a continuing risk to Plaintiffs and Tennessee Subclass members as well as to the general public.

1605. Plaintiffs and Tennessee Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

COUNT LXXI – DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT,
TEXAS BUS. & COM. CODE §§ 17.41, ET SEQ.
(ON BEHALF OF PLAINTIFFS BETHANN JACKSON AND MINOR STUDENTS C.J. AND M.J., ASIA PRITCHETT AND MINOR STUDENT B.M., AND FORMER STUDENT PLAINTIFF STEFAN SPANN, AND THE TEXAS SUBCLASS)

1606. Texas Plaintiffs Bethann Jackson and Minor Students C.J. and M.J., Asia Pritchett and Minor Student B.M., and Former Student Plaintiff Stefan Spann ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1607. Defendants are "persons" as defined by Tex. Bus. & Com. Code § 17.45(3).

1608. Plaintiffs and the Texas Subclass members are "consumers" as defined by Tex. Bus. & Com. Code § 17.45(4).

1609. Defendants advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas as defined by Tex. Bus. & Com. Code § 17.45(6).

1610. Defendants engaged in false, misleading, or deceptive acts and practices in violation of Tex. Bus. & Com. Code § 17.46(b), including:

(a) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

(b) Representing that goods or services are of a particular standard, quality or grade, if they are of another;

(c) Advertising goods or services with intent not to sell them as advertised.

1611. Defendants' false, misleading, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Texas Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Texas Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

1612. Defendants intended to mislead Plaintiffs and Texas Subclass members and induce them to rely on their misrepresentations and omissions.

1613. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1614. Had Defendants disclosed to Plaintiffs and Texas Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Texas Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Texas Subclass members paid without advising Plaintiffs and Texas Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Texas Subclass members' PII. Accordingly, Plaintiffs and the Texas Subclass members

acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1615. Defendants had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensiveness of the PII in their possession. This duty arose because Plaintiffs and the Texas Subclass members reposed trust and confidence in Defendants when they provided their PII to Defendants in exchange for Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

1616. Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendants engaged in acts or practices that, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1617. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively by Defendants. Consumers also lacked the ability, experience, or capacity to secure the PII in Defendants' possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in

information security matters and do not have access to Defendants' systems to evaluate their security controls. Defendants took advantage of their special skill and access to PII to hide their inability to protect the security and confidentiality of Plaintiffs' and Texas Subclass members' PII.

1618. Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Defendants' unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

1619. Defendants acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act and recklessly disregarded Plaintiffs' and Texas Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1620. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged

herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1621. Defendants' unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

1622. Defendants' violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

1623. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; restitution; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

COUNT LXXII – UTAH CONSUMER SALES PRACTICES ACT, UTAH CODE §§ 13-11-1, ET SEQ.
(ON BEHALF OF PLAINTIFFS JOSEPH HAUPTMAN AND MINOR STUDENTS D.H. AND M.H, FORMER STUDENT HAILEY MCCALL SHINGLETON, AND THE UTAH SUBCLASS)

1624. Utah Plaintiffs Joseph Hauptman and Minor Students D.H. and M.H., and Former Student Hailey McCall Shingleton, ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1625. Defendants are "persons" as defined by Utah Code § 13-11-1(5).

1626. Defendants are "suppliers" as defined by Utah Code § 13-11-1(6), because they regularly solicit, engage in, or enforce "consumer transactions" as defined by Utah Code § 13-11-1(2).

1627. Defendants engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Utah Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Utah Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Utah Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Utah Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Utah Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and

privacy of Plaintiffs' and Utah Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13- 44-201.

1628. Defendants intended to mislead Plaintiffs and Utah Subclass members and induce them to rely on their misrepresentations and omissions.

1629. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1630. Had Defendants disclosed to Plaintiffs and Utah Subclass members that their data systems were not secure and, thus, vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Utah Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Utah Subclass members paid without advising Plaintiffs and Utah Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Utah Subclass members' PII. Accordingly, Plaintiffs and the Utah Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1631. Defendants had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. This duty arose because Plaintiff and the Utah Subclass members reposed trust and confidence in Defendants when they provided their PII to Defendants in exchange for Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Utah Subclass—and Defendants because consumers are unable to fully protect their interests with regard to their data,

and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

1632. Defendants intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

(a) indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;

(b) indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if they are not;

(c) indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;

(d) indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g., more data security) than the supplier intends.

1633. Defendants engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Defendants' acts and practices unjustly imposed hardship on Plaintiffs and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity and cancelling and replacing passports; and lost value of their PII. The deficiencies in

Defendants' data security and the material misrepresentations and omissions concerning those deficiencies led to unfair surprise to Plaintiffs and the Utah Subclass when the data breach occurred.

1634. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required Defendants, as one of the educational software providers that collects, maintain, and compiles their customers' PII, to adequately secure PII in their possession. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiffs and the Utah Subclass, and Defendants, which has complete control over the PII in their possession.

1635. Defendants' acts and practices were also procedurally unconscionable because consumers, including Plaintiffs and the Utah Subclass, had no practicable option but to have their PII stored in Defendants' systems if they wanted to use Defendants' services. Defendants exploited this imbalance in power and the asymmetry of information about their data security to profit by inadequately securing the PII in their systems.

1636. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants, since they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1637. Defendants' violations present a continuing risk to Plaintiffs and Utah Subclass members as well as to the general public.

1638. Plaintiffs and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, et seq.; injunctive relief; and reasonable attorneys' fees and costs.

COUNT LXXIII – VERMONT CONSUMER FRAUD ACT, VT. STAT. ANN. TIT. 9, §§ 2451, ET SEQ. (ON BEHALF OF PLAINTIFF EMPLOYEE MICHELE BALLARDAND THE VERMONT SUBCLASS)

1639. Vermont Plaintiff Employee Michele Ballard ("Plaintiff," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1640. Plaintiff and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

1641. Defendants' conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

1642. Defendants are "sellers" as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

1643. Defendants advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

1644. Defendants engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Vermont Subclass members' PII, 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, and adequately improve security and privacy

measures following previous cybersecurity incidents, 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 Plaintiff's and Vermont Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Vermont Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Vermont Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Vermont Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Vermont Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1645. Defendants intended to mislead Plaintiff and Vermont Subclass members and induce them to rely on their misrepresentations and omissions.

1646. Defendants' representations and omissions were material because they were likely to deceive Plaintiff and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1647. Under the circumstances, consumers had a reasonable interpretation of Defendants' representations and omissions.

1648. Defendants had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. This duty arose because Plaintiff and the Vermont Subclass members reposed trust and confidence in Defendants when they provided their PII to Defendants in exchange for Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Vermont Subclass—and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiff and the Vermont Subclass that contradicted these representations.

1649. Defendants' acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1650. The injury to consumers was and is substantial because it was non-trivial and non- speculative; and involved a concrete monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1651. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an

obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1652. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

1653. Defendants are presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

1654. Defendants acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act and recklessly disregarded Plaintiff's and Vermont Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiff's and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1655. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiff and Vermont Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1656. Defendants' violations present a continuing risk to Plaintiffs and Vermont Subclass members as well as to the general public.

1657. Plaintiff and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

COUNT LXXIV – VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT,
VA. CODE. ANN. §§ 18.2-186.6, ET SEQ.
(ON BEHALF OF PLAINTIFFS TEACHER DUSTY SPENCE, ELEANOR TILLMAN AND MINOR STUDENT L.L., AND TOWFEQ ZARIF AND MINOR STUDENT P.Z., AND THE VIRGINIA SUBCLASS)

1658. Virginia Plaintiffs Teacher Dusty Spence, Eleanor Tillman and Minor Student L.L., and Towfeq Zarif and Minor Student P.Z. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1659. Defendants must accurately notify Plaintiffs and Virginia Subclass members following discovery or notification of a breach of their data security system if unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or they are reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

1660. Defendants are entities that own or license computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

1661. Plaintiffs' and Virginia Subclass members' PII includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

1662. Because Defendants discovered a breach of their security system in which unencrypted or unredacted Personal Information was or is reasonably believed to have

been accessed and acquired by an unauthorized person, who will, or they are reasonably believed who will, engage in identify theft or another fraud, Defendants were obligated to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

1663. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Va. Code Ann. § 18.2-186.6(B).

1664. As a direct and proximate result of Defendants' violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

1665. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT LXXV – VIRGINIA CONSUMER PROTECTION ACT, VA. CODE ANN. §§ 59.1-196, ET SEQ. (ON BEHALF OF PLAINTIFFS TEACHER DUSTY SPENCE, ELEANOR TILLMAN AND MINOR STUDENT L.L., AND TOWFEQ ZARIF AND MINOR STUDENT P.Z., AND THE VIRGINIA SUBCLASS)

1666. Virginia Plaintiffs Teacher Dusty Spence, Eleanor Tillman and Minor Student L.L., and Towfeq Zarif and Minor Student P.Z. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1667. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

1668. Defendants are "persons" as defined by Va. Code Ann. § 59.1-198.

1669. Defendants are "suppliers" as defined by Va. Code Ann. § 59.1-198.

1670. Defendants engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Defendants advertised, offered, or sold goods or services used

primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment.

1671. Defendants engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Virginia Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Virginia Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Virginia Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Virginia Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Virginia Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and

privacy of Plaintiff and Virginia Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1672. Defendants intended to mislead Plaintiffs and Virginia Subclass members and induce them to rely on their misrepresentations and omissions.

1673. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members, including Plaintiffs and Virginia Subclass members, about the adequacy of Defendants' computer and data security and the quality of the Defendants brand.

1674. Had Defendants disclosed to Plaintiffs and Virginia Subclass members that their data systems were not secure and thus were vulnerable to attack, Defendants could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Virginia Subclass members' PII as part of the services Defendants provided and for which Plaintiffs and Virginia Subclass members paid without advising Plaintiffs' and Virginia Subclass members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Virginia Subclass members' PII. Accordingly, Plaintiffs and the Virginia Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

1675. In addition, Defendants had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. Such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Virginia Subclass—and Defendants because consumers are unable to fully protect their interests with regard to their data and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiffs and the Virginia Subclass that contradicted these representations.

1676. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

(a) Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

(b) Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

(c) Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

1677. Defendants acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act and recklessly disregarded Plaintiff and Virginia Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate. An award of punitive damages would serve to punish Defendants for their wrongdoing and warn or deter others from engaging in similar conduct.

1678. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiffs and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would

not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1679. Defendants' violations present a continuing risk to Plaintiffs and Virginia Subclass members as well as to the general public.

1680. Plaintiffs and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

COUNT LXXVI - WASHINGTON DATA BREACH NOTICE ACT, WASH. REV. CODE §§ 19.255.010, ET SEQ.
(ON BEHALF OF PLAINTIFFS EMILY PEASE AND MINOR STUDENTS A.E.J.A., A.R.R., AND A.E.R., HEATHER TAYLOR AND MINOR STUDENTS B.N.T. AND B.A.T., AND THE WASHINGTON SUBCLASS)

1681. Washington Plaintiffs Emily Pease and Minor Students A.E.J.A., A.R.R., and A.E.R. and Heather Taylor and Minor Students B.N.T. and B.A.T. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1682. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Wash. Rev. Code § 19.255.010(1).

1683. Plaintiffs' and Washington Subclass members' PII includes Personal Information as covered under Wash. Rev. Code § 19.255.010(5).

1684. Under Wash. Rev. Code § 19.255.010(1), Defendants must accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of their data security system if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, in the most expedient time possible and without unreasonable delay.

1685. Because Defendants discovered a breach of their security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

1686. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Wash. Rev. Code § 19.255.010(1).

1687. As a direct and proximate result of Defendants' violations of Wash. Rev. Code § 19.255.010(1), Plaintiffs and Washington Subclass members suffered damages, as described above. 1260. Plaintiffs and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

COUNT LXXVII – WASHINGTON CONSUMER PROTECTION ACT, WASH. REV. CODE ANN. §§ 19.86.020, ET SEQ.
(ON BEHALF OF PLAINTIFFS EMILY PEASE AND MINOR STUDENTS A.E.J.A., A.R.R., AND A.E.R., HEATHER TAYLOR AND MINOR STUDENTS B.N.T. AND B.A.T., AND THE WASHINGTON SUBCLASS)

1688. Washington Plaintiffs Emily Pease and Minor Students A.E.J.A., A.R.R., and A.E.R. and Heather Taylor and Minor Students B.N.T. and B.A.T. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1689. Defendants are "persons" as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1690. Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1691. Defendants engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Washington Subclass members' PII, 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, and adequately improve security and privacy measures after previous cybersecurity incidents, 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 Washington Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Washington Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Washington Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Washington Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Washington Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1692. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1693. Defendants acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act and recklessly disregarded Plaintiffs' and Washington Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1694. Defendants' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, their conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

1695. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for

credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1696. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

COUNT LXXVIII – NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION,
WIS. STAT. §§ 134.98(2), ET SEQ.
(ON BEHALF OF PLAINTIFFS MICHELLE LA COUNT AND MINOR STUDENTS E.R.M. AND R.E.M. AND FORMER STUDENT KAYELEEN CAMPBELL, AND THE WISCONSIN SUBCLASS)

1697. Wisconsin Plaintiffs Michelle La Count and Minor Students E.R.M. and R.E.M. and Former Student Kayeleen Campbell ("Plaintiff," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1698. Defendants are businesses that maintain or license Personal Information as defined by Wis. Stat. § 134.98(2).

1699. Plaintiff's and Wisconsin Subclass members' PII includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

1700. Under Wis. Stat. §§ 134.98(2)-(3)(a), Defendants must accurately notify Plaintiff and Wisconsin Subclass members if they know that PII in their possession has been acquired by a person whom it has not authorized to acquire the PII within a reasonable time.

1701. Because Defendants knew that PII in their possession had been acquired by a person whom it had not authorized to acquire the PII, Defendants had an obligation

to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

1702. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Wis. Stat. § 134.98(2).

1703. As a direct and proximate result of Defendants' violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

1704. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT LXXIX – WISCONSIN DECEPTIVE TRADE PRACTICES ACT, WIS. STAT. § 100.18

(ON BEHALF OF PLAINTIFFS FORMER STUDENT KAYELEEN CAMPBELL, MICHELLE LA COUNT AND MINOR STUDENTS E.R.M. AND R.E.M., AND THE WISCONSIN SUBCLASS)

1705. Wisconsin Plaintiff Former Student Kayeleen Campbell and Michelle La Count and Minor Students E.R.M. and R.E.M. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1706. Defendants are each a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

1707. Plaintiffs and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

1708. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Defendants to members of the public for sale, use, or distribution, Defendants made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations

to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1709. Defendants also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1710. Defendants' deceptive acts, practices, plans, and schemes include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Wisconsin Subclass members' PII, 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, and adequately improve security and privacy measures following previous cybersecurity incidents, 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 Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Wisconsin Subclass members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy Plaintiffs' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Wisconsin Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1711. Defendants intended to mislead Plaintiffs and Wisconsin Subclass members and induce them to rely on their misrepresentations and omissions.

1712. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

1713. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensiveness of the PII in their possession. This duty arose because Plaintiffs and the Wisconsin Subclass members reposed trust and confidence in Defendants when they provided their PII to Defendants in exchange for Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Wisconsin Subclass—and Defendants because consumers are unable to fully protect their interests with regard to their data and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

1714. Defendants' failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1715. Defendants acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act and recklessly disregarded Plaintiffs' and Wisconsin Subclass members' rights. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1716. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiffs and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

1717. Defendants had an ongoing duty to all Defendants customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

1718. Plaintiffs and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

COUNT LXXX – COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS,
WYO. STAT. ANN. §§ 40-12-502(A), ET SEQ.
(ON BEHALF OF PLAINTIFFS SKYE BREANN LAWSON AND MINOR STUDENTS B.L. AND H.L. AND THE WYOMING SUBCLASS)

1719. Wyoming Plaintiffs Skye Breann Lawson and Minor Students B.L. and H.L. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1720. Defendants are businesses that own or license computerized data that includes personal identifying information as defined by Wyo. Stat. Ann. § 40-12-502(a).

1721. Plaintiffs' and Wyoming Subclass members' PII includes personal identifying information as covered under Wyo. Stat. Ann. § 40-12-502(a).

1722. Pursuant to Wyo. Stat. Ann. § 40-12-502(a), Defendants were required to accurately notify Plaintiffs and Wyoming Subclass members of the Data Breach in the most expedient time possible and without unreasonable delay.

1723. Because Defendants were aware of a breach of its data security system in which the misuse of personal identifying information has occurred or is reasonably likely to occur, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

1724. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Wyo. Stat. Ann. § 40-12-502(a).

1725. As a direct and proximate result of Defendants' violations of Wyo. Stat. Ann. § 40- 12-502(a), Plaintiffs and Wyoming Subclass members suffered damages, as described above.

1726. Plaintiffs and Defendants Subclass members seek relief under Wyo. Stat. Ann. § 40- 12-502(f), including actual damages and equitable relief.

COUNT LXXXI – WYOMING CONSUMER PROTECTION ACT, WYO. STAT. ANN. §§ 40-12-101, ET SEQ.
(ON BEHALF OF PLAINTIFFS SKYE BREANN LAWSON AND MINOR STUDENTS B.L. AND H.L. AND THE WYOMING SUBCLASS)

1727. Wyoming Plaintiffs Skye Breann Lawson and Minor Students B.L. and H.L. ("Plaintiffs," for purposes of this Count) repeat and re-allege the factual allegations above as if fully set forth herein.

1728. Defendants are "persons" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(i).

1729. Defendants' goods and services are "merchandise" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(vi).

1730. Defendants engage in "consumer transactions" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(ii).

1731. Defendants have "advertised" their goods and services within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(v).

1732. Plaintiffs sent a demand for relief on behalf of the Wyoming Subclass pursuant to Wyo. Stat. Ann. § 40-12-109 on July 11, 2025. Defendants have not cured the deceptive trade practices described below.

1733. Defendants knowingly engaged in unfair and deceptive trade practices in the course of their business and in connection with consumer transactions, including by:

(a) Failing to implement and maintain reasonable security measures to protect Plaintiffs' and Wyoming Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

(b) Failing to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents;

(c) Failing to comply with common law and statutory duties pertaining to the security of Plaintiffs' and Wyoming Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(d) Misrepresenting that they would implement and maintain reasonable security measures to protect Plaintiffs' and Wyoming Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security of Plaintiffs' and Wyoming Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(f) Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Wyoming Subclass members' PII; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security of Plaintiffs' and Wyoming Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1734. Through the above-described conduct, Defendants violated Wyo. Stat. Ann. § 40-12- 105(a) by:

(a) Knowingly representing that goods or services have sponsorship, approval, accessories or uses they do not have;

(b) Knowingly representing that goods or services are of a particular standard or grade, if they are not;

(c) Knowingly representing that goods or services have been supplied in accordance with a previous representation, if they have not;

(d) Knowingly advertising goods or services with intent not to sell them as advertised; and

(e) Knowingly engaging in unfair or deceptive acts or practices.

1735. Defendants intentionally made the above-described representations and omissions of material fact with knowledge of their falsity or reckless disregard of the truth. Defendants knew or should have known that their computer systems and data security practices were inadequate to protect Plaintiffs' and Wyoming Subclass members' PII and that a data breach or theft was highly likely to occur. Defendants (1) represented in their information privacy and confidentiality policies that they were implementing reasonable security measures to protect Plaintiffs' and Class Members' sensitive personal information and (2) failed to implement reasonable data security measures, including reducing and outsourcing cybersecurity personnel, despite being on notice that their data security and privacy protections were inadequate.

1736. In making their representations and omissions, Defendants intended to mislead Plaintiffs and Wyoming Subclass members and cause them to act or elect not to act based on these representations and omissions. Defendants knew or should have known that their conduct violated Wyo. Stat. § 40-12-105.

1737. Defendants' representations and omissions were material because they were likely to deceive Plaintiffs and Class Members, including Plaintiffs and Wyoming Subclass members, about the adequacy of Defendants' computer and data security and the quality of the Defendants brand.

1738. Plaintiffs and Wyoming Subclass members were ignorant of the falsity of Defendants' representations and omissions and relied on these representations and omissions in choosing to act or not act.

1739. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the PII in their possession. This duty arose because Plaintiffs and the Wyoming Subclass members reposed a trust and confidence in Defendants when they provided their PII to Defendants in exchange for Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff

and the Wyoming Subclass—and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from their general duty to exercise reasonable care and their knowledge that Plaintiffs and Wyoming Subclass members might justifiably be induced by Defendants' omissions to act or refrain from acting in a business transaction. Additionally, Defendants had a duty to disclose inadequacies in their data security because such facts were basic to the transactions in question; Defendants knew Plaintiff and Wyoming Subclass members were mistaken as to these facts, would enter transactions as a result, and—based on objective circumstances—would reasonably expect a disclosure of those facts. Defendants' duty to disclose also arose from its:

(a) Possession of exclusive knowledge regarding the security of the data in their systems;

(b) Active concealment of the state of their security; and/or

(c) Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiffs and the Wyoming Subclass that contradicted these representations.

1740. As described above, Defendants' statements and omissions were likely to deceive a reasonable consumer because consumers provided their PII to Defendants in exchange for Defendants' services and because Defendants kept the inadequate state of their security controls secret from the public. In light of their direct relationship with their customers, Defendants' statements concerning data security constitute representations that their security was, at minimum, reasonable.

1741. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by

consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1742. The injury to consumers from Defendants' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1743. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1744. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

1745. As a direct and proximate result of Defendants' uncured unfair and deceptive acts or practices, Plaintiffs and Wyoming Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and/or non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity and cancelling and replacing passports; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

1746. Plaintiffs and Wyoming Subclass members seek relief pursuant to Wyo. Stat. Ann. § 40-12-108, including damages and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly

situated, request that this Court:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23;

B. Order appropriate compensatory, statutory, punitive, and nominal damages to Plaintiffs and Class Members under applicable law;

C. Order appropriate injunctive, equitable, and declaratory relief under applicable law;

D. Award Plaintiffs an appropriate Class representative service award for their prosecution of this matter on behalf of all Class members;

E. Award Plaintiffs and the Class pre-judgement and/or post-judgment interest as prescribed by law;

F. Award reasonable attorneys' fees and costs as permitted by law; and

G. Enter other and further relief as the Court deems to be both just and fair.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: August 11, 2025

Respectfully submitted,

[*Signature blocks on following page*]

/s/ James J. Pizzirusso
James J. Pizzirusso, D.C. State Bar No. 477604*
jpizzirusso@hausfeld.com
HAUSFELD LLP
1200 17th Street, N.W., Suite 600
Washington, DC 20036
Tel.: (202) 540-7200

Co-Lead Counsel for Individual Action Plaintiffs (Track One)

/s/ David S. Casey, Jr.
David S. Casey, Jr., Cal. State Bar No. 60768
dcasey@cglaw.com
CASEY GERRY
FRANCAVILLA BLATT LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811

Co-Lead Counsel for Class Action Plaintiffs (Track One)

/s/ Carol C. Villegas
Carol C. Villegas, N.Y. State Bar No. 4154324*
cvillegas@labaton.com
LABATON KELLER SUCHAROW LLP
140 Broadway
New York, New York 10005
Tel.: (212) 907-0700
Co-Lead Counsel for Teachers Unions Plaintiffs (Track One)