

1 JOSEPH W. COTCHETT (SBN 36324)  
2 ZACHARY ZAHAROFF (SBN 321878)  
3 **COTCHETT, PITRE & McCARTHY, LLP**  
4 840 Malcolm Rd.  
5 Burlingame, CA 94010  
6 Telephone: (650) 697-6000  
7 Facsimile: (650) 697-0577

8 KARIN SWOPE (pro hac vice forthcoming)  
9 ANDREW J. FULLER (pro hac vice forthcoming)  
10 KELLY A. ARISTIDES (SBN 357856)  
11 **COTCHETT, PITRE & McCARTHY, LLP**  
12 1809 7th Avenue, Suite 1610  
13 Seattle, WA 98101  
14 Telephone: (206) 802-1272  
15 Facsimile: (206) 299-4184

16 *Attorneys for Plaintiffs and the Proposed Class*

17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
**UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA**

18 TIANA CHAMBERLAIN, on behalf of K.J.K. and  
19 K.J.K, and ADAM SIMSON, individually, and on  
20 behalf of all others similarly situated,

21 Plaintiffs,

22 v.

23 EDUCATIONAL TESTING SERVICE,

24 Defendant.

Case No. 26-cv-12217

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

1 Plaintiffs K.J.K. and K.J.K., minors, by and through their parent Tiana Chamberlain,<sup>1</sup> and  
2 Plaintiff Adam Simson, individually, and on behalf of all others similarly situated, hereby file suit  
3 against Defendant Educational Testing Service and allege the following based on personal knowledge,  
4 information and belief, the investigation of counsel, and public sources:

## 5 I. INTRODUCTION

6 1. On October 16, 2026, the California Department of Education announced that students  
7 at California public schools, and former students who graduated within the past three years, have been  
8 victims of a massive data breach at Defendant Educational Testing Service (“ETS”).<sup>2</sup> Public reporting  
9 estimates that the victim population is roughly 7 million people.<sup>3</sup>  
10

11 2. ETS is one of the most influential companies in global education and one of the most  
12 prominent and powerful players in the standardized testing industry. It reaches into almost every aspect  
13 of testing in the United States and has obtained an extraordinary amount of data on young people  
14 throughout California.

15 3. According to ETS, it has “produced more than 180 test titles, including the National  
16 Assessment of Educational Progress (NAEP) for the U.S. Department of Education, the AP<sup>®</sup> and the  
17 SAT<sup>®</sup> tests for the College Board<sup>®</sup>, as well as state and district assessments.”<sup>4</sup> In 2024, ETS stopped  
18 administering the SAT test. On June 30, 2026, ETS announced it was acquiring the ACT, the major  
19

---

22 <sup>1</sup> Pursuant to Federal Rule of Civil Procedure 5.1(a)(3), this Complaint uses initials for minor Plaintiffs.  
23 However, because the minor Plaintiffs have the same initials, the Complaint will hereinafter refer to  
24 them respectively as K.J.K.-1 and K.J.K.-2.

25 <sup>2</sup> Eric He and Tyler Katzenberger, *Hack exposes data on millions of California students*, Politico, Oct.  
26 16, 2026, <https://www.politico.com/news/2026/10/16/hack-exposes-data-on-millions-of-california-students-01124018> (last visited Oct. 17, 2026).

27 <sup>3</sup> *Id.*

28 <sup>4</sup> ETS K-12 Student Assessment Programs, <https://www.ets.org/k12/capabilities/assessment-development.html> (last viewed Oct. 17, 2026).

competitor to the SAT.<sup>5</sup> ETS exams also include the Graduate Record Exam (the GRE), the Test of English as a Foreign Language (TOEFL), the Praxis Series, a teacher licensing and certification examination, and K-12 statewide accountability assessments that it develops and offers to state departments of education.

4. The victims also face serious and substantial social and emotional consequences from their loss of control over information about their physical and mental health conditions.

5. California parents and students entrusted ETS with sensitive and valuable information. ETS was fully aware of the value and sensitivity of that information, yet failed to adequately protect it. ETS failed to protect and safeguard Plaintiffs' and Class Members' Personally Identifiable Information ("PII") and Protected Health Information (PHI). This PII and PHI was compromised due to Defendant's negligent or careless acts and omissions. Hackers targeted and obtained Plaintiffs and Class Members' PII and PHI because of its value in exploiting and stealing Plaintiffs and Class Members' identities. The current and continuing risk to victims of this breach, including Plaintiffs and Class Members, will remain for their lifetimes.

6. Due to this breach and ETS' failures, Plaintiffs and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for decades. Plaintiffs and Class Members must now and in the future closely monitor and guard against identity theft at their own expense. Plaintiffs and Class Members will accordingly face continuing out-of-pocket expenses, including credit reports, credit monitoring services, credit freezes, or other protective measures to deter, detect, and safeguard against identity theft.

7. Plaintiffs file this Complaint to remedy these harms to themselves and to all similarly situated individuals whose PII and PMI were accessed during the data breach.

---

<sup>5</sup> Press Release, "ETS Acquires ACT, Expanding Pathways to Opportunity Across America," June 30, 2026, <https://www.ets.org/newsroom/ets-acquires-act.html> (last visited Oct. 17, 2026).

## II. PARTIES

### A. Plaintiffs

8. Plaintiff K.J.K.-1 is a minor and brings her claims through her parent, Tiana Chamberlain. Plaintiff K.J.K.-1 and Tiana Chamberlain are citizens of Fortuna, California. Plaintiff K.J.K.-1 is 12 years old and currently enrolled in a public elementary school in Fortuna, CA, in Humboldt County.

9. Plaintiff K.J.K.-2 is a minor and brings his claims through his parent, Tiana Chamberlain. Plaintiff K.J.K.-2 and Tiana Chamberlain are citizens of Fortuna, California. Plaintiff K.J.K.-2 is 10 years old and currently enrolled in a public elementary school in Fortuna, CA, in Humboldt County.

10. Plaintiff Adam Simson is a citizen of Glenn, California. He graduated in 2026 from a public high school in Hamilton City, California.

### B. Defendant

11. Defendant Educational Testing Service is a non-profit corporation organized under the laws of the state of New York, with a principal place of business located in Princeton, New Jersey. Educational Testing Service is registered to do business in California.

## III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars (\$5,000,000.00), there are in excess of 100 Class members, the action is a class action in which one or more Class members are citizens of states different from Defendants.

13. The Court has personal jurisdiction over Defendant ETS because ETS purposefully availed itself of the privilege of conducting activities in California. These activities included, but were not limited to, the provision of services related to the educational assessment and testing of millions of Californians. Plaintiffs' claims arise out of or relate to ETS' contacts with California.

14. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, were directed to, and/or emanated from this District; Defendant transacts substantial business and has agents in this District; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District.

15. **Divisional Assignment.** Pursuant to Local Rule 3-5(b) and 3-2(f), this matter should be assigned to the Eureka Division given that a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, or were directed to, Humboldt County.

#### IV. FACTUAL ALLEGATIONS

##### A. ETS Collects PII and PHI From California Students.

16. ETS does extensive work for the California Department of Education. This includes, but is not limited to, “[d]elivering statewide assessments for six million K–12 public school students and serving as the designated contractor on the California Assessment of Student Performance and Progress (CAASPP) and the English Language Proficiency Assessments for California (ELPAC).”<sup>6</sup> The CAASPP includes, but is not limited to, the California Science Test, the California Alternative Assessments for students with cognitive disabilities, and the California Spanish Assessment.<sup>7</sup>

17. According to the California Department of Education, “ETS provides all services required to develop, deliver, and report the CAASPP and ELPAC. Services include item and test development; LEA[, Local Educational Agencies,] training and training resources; LEA support services; psychometric services; technology services to support computer-based testing; analysis and scoring; and student-, LEA-, and state-level reporting.”<sup>8</sup>

---

<sup>6</sup> See *supra* n. 3.

<sup>7</sup> California Department of Education, “About the California Assessment System,” <https://www.caaspp-elpac.org/about> (last visited Oct. 17, 2026).

<sup>8</sup> *Id.*

1           18. As part of its work handling America’s testing apparatus, ETS handles extremely  
2 sensitive data on the intellectual development and disabilities of minors across the United States,  
3 including in California. The company reviews requests for accommodations and evaluates the extremely  
4 sensitive information submitted to determine whether a child has a disability and, if so, what type of  
5 accommodation may be appropriate. ETS has different guidelines for what it requires to assess disability  
6 claims and has disability-specific requirements for conditions including, but not limited to:

- 7           (1) ADHD;  
8           (2) Autism Spectrum Disorder;  
9           (3) Intellectual Disabilities;  
10           (4) Learning Disabilities;  
11           (5) Physical Disabilities and Chronic Health Conditions;  
12           (6) Traumatic Brain Injuries; and  
13           (7) Psychiatric Disabilities.

14           19. Although ETS does not independently conduct medical assessments of California  
15 minors, it obtains, reviews, and stores documentation from those medical assessments as part of its  
16 determination of whether a student is entitled to an accommodation, and if so, what kind of  
17 accommodation is appropriate.  
18  
19

20           **B. As a Result of Its Negligence and Carelessness, ETS Experienced a Data Breach that**  
21           **Exposed the PII and PHI of Millions of California Students.**

22           20. On October 16, 2026, the California Department of Education announced that ETS  
23 experienced a massive data breach. The breach involved the exfiltration of highly sensitive data  
24 pertaining to millions of minors as well as adults. The breach included data pertaining “current and  
25 former students enrolled in California public schools between 2023 and the current school year, as well  
26  
27  
28

1 as students who left a California school since 2006 and did not confirm transfer to another school with  
2 the CDE.”<sup>9</sup>

3 21. Accordingly, the breach appears to include the data of at least the following groups:

- 4 (1) minors currently enrolled in a California public school;
- 5 (2) minors currently enrolled in a California private school, but who either were  
6 enrolled in California public school between 2023 and the current school year or  
7 who left a California public school at any time since 2006 but not confirm their  
8 transfer with the California Department of Education;
- 9 (3) minors currently enrolled in public or private schools elsewhere in the United  
10 States but who either were enrolled in California public school between 2023 and  
11 the current school year or who left a California public school at any time since  
12 2006 but not confirm their transfer with the California Department of Education;  
13 and  
14 (4) adults who are no longer enrolled in a California public school but were enrolled  
15 in a California public school between 2023 and the current school year or who  
16 left a California public school at any time since 2006 but did not confirm their  
17 transfer with the California Department of Education.  
18  
19

20 22. ETS claims that it first discovered the data breach on September 25, 2026, the date on  
21 which it “identified unauthorized activity involving an SFTP site used to exchange California statewide  
22 assessment information with CDE.”<sup>10</sup> It has also stated that, with the assistance of outside experts, it  
23 learned that the hacker “used a compromised login credential at various times during the period from  
24

25 \_\_\_\_\_  
26 <sup>9</sup> California Department of Education, *Educational Testing Service (ETS) Incident*,  
<https://www.cde.ca.gov/nr/in/ets-incident.asp#formerstudents> (last visited Oct. 17, 2026).

27 <sup>10</sup> ETS, *Notification of Data Breach*, <https://www.cde.ca.gov/nr/in/ets-notification.asp> (last visited Oct.  
28 17, 2026).

1 May 22, 2026 to September 18, 2026 to access the SFTP site to copy files containing California student  
 2 information.”<sup>11</sup>

3 23. ETS has provided no explanation for the discrepancy between ETS’ claim that September  
 4 18, 2026 was the end date of the hacker’s exploitation of access and ETS’ claim that it “identified  
 5 unauthorized activity” on September 26, 2026, the date on which ETS claims to have learned of the  
 6 breach.

7 24. This data breach did not need to happen. It was caused by ETS’ failure to take reasonable  
 8 measures to protect the data of California students. The California Department of Education stated that  
 9 the breach involved “unauthorized access to and copying of student data from an ETS secure file transfer  
 10 protocol (SFTP) site.”<sup>12</sup> The California Department of Education further disclosed that “an  
 11 unauthorized party used a compromised login credential at various times during the period from May  
 12 22, 2026 to September 18, 2026 to access the SFTP site to copy files containing California student  
 13 information.”  
 14

15 25. ETS failed to take reasonable measures to protect California students and former students  
 16 and that failure caused the breach. As discussed further below, there are many reasonable measures that  
 17 ETS should have taken, and failed to take, that would have prevented this breach and the compromise  
 18 of login credentials. As Anton Dahbura, Executive Director of the Johns Hopkins University  
 19 Information Security Institute stated to the Los Angeles Times:  
 20

21 A stolen login credential should not become a months-long passport to millions of  
 22 students’ personal records. If that is what happened here, the critical question is why  
 23 authentication safeguards, access restrictions, and monitoring systems failed to detect  
 24 and stop the unauthorized activity.<sup>13</sup>

25 <sup>11</sup> *Id.*

26 <sup>12</sup> California Department of Education, Educational Testing Service (ETS) Notification,  
<https://www.cde.ca.gov/nr/in/ets-notification.asp> (last visited Oct. 17, 2026).

27 <sup>13</sup> Howard Blume, Andrew Khouri, and Jaweed Kaleem, *Hackers steal personal data of California*  
 28 *students in massive breach*, Los Angeles Times, Oct. 16, 2026, <https://www.latimes.com/>

1           26.     ETS also failed to take reasonable measures to adequately monitor its own systems.  
2 According to ETS, the hacker had access to ETS' systems—undetected—for months. ETS claims that  
3 the hacker first exploited its access on May 22, 2026 and that ETS first detected “unauthorized activity”  
4 on September 26, 2026. Accordingly, ETS failed to detect the hacker for approximately 5 months. If  
5 ETS had employed adequate and reasonable access, intrusion detection, and network monitoring  
6 systems and protocols, the breach would have been detected and halted far sooner.

7  
8           27.     The PII that the ETS failed to safeguard and which has been exfiltrated is extensive and  
9 sensitive. It includes names, birth dates, home addresses, grade levels, school information, statewide  
10 and local student ID numbers, detailed demographic information about students, information on race,  
11 gender, ethnicity, primary language, country of origin, and English learner status and English language  
12 proficiency. The breach also includes information obtained from the assessments themselves, as well as  
13 data related to a student's eligibility to participate in programs for students with ties to the United States  
14 military and programs for impoverished, migrant, abandoned, or homeless youth. And finally, the data  
15 released includes information on disabilities and medical conditions, including, but not limited to, data  
16 on individuals' mental and physical disabilities, accommodation statuses, and status under Section 504  
17 of U.S. Rehabilitation Act of 1973 (“Section 504”), which pertains in part to persons with certain  
18 physical and mental impairments.  
19

20  
21           28.     This stolen data is extremely sensitive. It links a student's name, home address, and date  
22 of birth to a persistent state-issued identifier. It also links it to confidential disability, educational,  
23 demographic, and program-eligibility information.

24           29.     ETS' breach also caused victims to lose control over, and face public exposure of, highly  
25 sensitive information on medical conditions, including data on disabilities. This breach will have long-  
26

27 \_\_\_\_\_  
28 [california/story/2026-10-16/state-testing-student-data-hack](https://www.sacramentobee.com/california/story/2026-10-16/state-testing-student-data-hack) (last visited Oct. 17, 2026).

1 lasting implications for exposure to medical billing fraud and criminals impersonating victims in  
2 government benefit programs.

3 30. The minors and adults affected by this breach will face the consequences for years. Data  
4 breaches can have extraordinarily serious consequences for their victims because they empower  
5 criminals to personate the victims and cause financial havoc. Data breaches allow the perpetrators to  
6 commit phone or utilities fraud, credit card fraud, or bank fraud, take out loans under victims' identities,  
7 commit medical identity theft, collect government benefits under victims' identifies, obtain driver's  
8 licenses or official identification cards in victims' names but with the criminals' photos, and file state  
9 or federal tax returns as the victim.<sup>14</sup> And PHI is particularly vulnerable: criminals commonly use PHI  
10 to commit a wide variety of offenses, including medical fraud. This is in large part why such a large and  
11 active cyber black market exists in which criminals exploit PHI on the dark web. Although PII sells for  
12 as little as \$1-\$2 on the black market, PHI sells for as much as \$363.<sup>15</sup>

14 31. The minors and young adults involved in this breach are particularly vulnerable because  
15 they may not yet have financial literacy or life experience with handling credit card bills, government  
16 benefits, driver licenses, credit scores, and obtaining medical services. A child's name, date of birth, and  
17 home address are foundational to constructing their adult identity. Because children usually lack credit  
18 records, criminals and their enterprises can use data like the information obtained in this breach to open  
19 various types of accounts and build fake identities. It may be years before they open their first bank  
20 account or credit card or otherwise first learn that criminals exploited their data to impersonate them and  
21 create massive complications to their livelihoods.  
22  
23  
24  
25

---

26 <sup>14</sup> McAfee, *A Guide to Identity Theft Statistics for 2026*, [https://www.mcafee.com/learn/a-guide-to-](https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics/)  
27 [identity-theft-statistics/](https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics/) (last visited Oct. 8, 2026).

28 <sup>15</sup> Center for Internet Security, *Data Breaches: In the Healthcare Sector*, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited Oct. 18, 2026).

1           32. Plaintiffs and Class Members have also been, and will continue to be, forced to put  
2 significant time and effort to attempt to contain the impact of this breach, including by verifying the  
3 legitimacy of communications about the data breach. monitoring accounts and credit data, changing  
4 account access controls and passwords, and researching the breach itself. Plaintiffs and Class Members  
5 will be required to do this for years in order to protect against identity theft and fraudulent misuse of the  
6 PII and PHI that ETS carelessly and negligently left exposed. The data breach also diminished the value  
7 of Plaintiffs and Class Members' PII and PHI, which are types of intangible property.

8           33. Plaintiffs and Class Members also remain at imminent risk of serious harm from ETS'  
9 inadequate data security practices. Plaintiffs and Class Members' PHI and PII are at substantial and  
10 imminent risk given ETS' failure to implement reasonable data security practices and procedures. For  
11 example, any data pertaining to Plaintiffs and Class Members that was not part of this breach could be  
12 exposed given ETS' data security failures. On information and belief, Plaintiffs and Class Members  
13 continue to have PHI and PII in ETS' custody and control that are inadequately safeguarded against  
14 known dangers and threats.

15           34. Plaintiffs and Class Members have also experienced substantial anxiety, worry, and  
16 emotional distress from the breach. Plaintiffs and Class Members are afraid given the identity theft and  
17 fraud consequences from the breach and because of the continuing uncertainty regarding the breach.  
18 Plaintiffs and Class Members are also experiencing fear and anxiety given the uncertainty about whether  
19 ETS is continuing to fail to reasonably protect Plaintiffs and Class Members' PII and PHI.

20           35. ETS was fully aware of its duty and obligation to safeguard the PII and PHI of Plaintiffs  
21 and Class Members both before and during the data breach. Despite this, ETS failed to protect Plaintiffs  
22 and Class Members' PII and PHI. ETS was also aware that the hacking of the data of Plaintiffs and Class  
23 Members would result in the injuries to Plaintiffs and Class Members alleged in this Complaint.

24           **C. ETS Made False Promises to Californians About the Security of Their Data and**  
25           **Obtained Access to Their PII and PHI Under False Pretenses.**  
26

1           36.     ETS obtains the PII and PHI of California students as a result of its data security promises  
2 to the public, including the victims of this data breach and their parents. In fact, ETS posts a “Special  
3 Notice to California Residents” on its webpage.<sup>16</sup> The “Special Notice to California Residents” advises  
4 Californians, including the victims of this data breach and their parents, that the company has “a global  
5 privacy program that protects your Personal Information no matter how or where it is collected, used or  
6 stored.”

7           37.     ETS also issued a K-12 Student Data Privacy Statement, which represents that ETS  
8 “protects K-12 Student Data at all times using appropriate security measures, including encryption,” and  
9 that ETS “does not retain K-12 Student Data longer than needed to fulfill the educational purposes for  
10 which it was collected.”<sup>17</sup>

11           38.     ETS violated its promises to Californians, including Plaintiffs and Class Members. Given  
12 ETS’ failure to employ rudimentary data security practices, technologies, protocols, and procedures that  
13 would have prevented this breach or timely detected it, there is no “global privacy program” that  
14 “protects your Personal Information no matter how or where it is collected, used or stored.” ETS also  
15 does not “protect[] K-12 Student Data at all times using appropriate security measures.” And given the  
16 scope of the data exfiltrated, including for persons who have already graduated from California public  
17 schools, ETS does retain K-12 Student Data for “longer than needed to fulfill the educational purposes  
18 for which it was collected.”

19           39.     Plaintiffs and Class Members had the reasonable expectation that ETS would comply  
20 with its obligations related to their PII and PHI. ETS owed Plaintiffs and Class Members a duty to  
21 provide reasonable security, consistent with industry standards and requirements, and to ensure that their  
22  
23  
24  
25

---

26 <sup>16</sup> ETS, “Special Notice to California Residents,” <https://www.ets.org/legal/privacy.html#accordion-1f944a369f-item-60dcfb5461> (last visited Oct. 17, 2026).

27 <sup>17</sup> ETS, “K-12 Student Data Privacy Statement,” <https://www.ets.org/legal/privacy/k-12-student-data-privacy-statement.html> (last visited Oct. 18, 2026).  
28

1 computer systems, networks, and data security practices, protocols, and procedures adequately protected  
2 their PII and PHI. The data breach resulted from ETS' failure to comply with its obligations.

3 40. Upon information and belief, ETS' contracts with the state of California or any political  
4 divisions or subdivisions thereof, including, but not limited to, the California Department of Education  
5 or any California school districts or municipalities, require ETS to protect and safeguard the PII and PHI  
6 of Californians, including, but not limited to, Plaintiffs and Class Members. Plaintiffs and Class  
7 Members are the intended third-party beneficiaries of those contracts and their data security promises  
8 and provisions, which are intended to ensure the security of Plaintiffs and Class Members' own PII and  
9 PHI.  
10

11 **D. ETS Failed to Abide by Regulatory Guidance and Implement Industry Standard**  
12 **Cybersecurity Practices and Procedures.**

13 41. ETS' failure to comply with federal and state laws and requirements and industry  
14 standards relating to securing PII and PHI is the cause of ETS' data security failures and the data breach  
15 itself.

16 42. ETS ignored and failed to abide by the Federal Trade Commission's ("FTC") guidance  
17 on industry-standard cybersecurity practices and the safeguarding of data. Section 5 of the FTC Act, 15  
18 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the  
19 FTC, failing to use reasonable measures to protect PII by companies like Defendants. According to the  
20 FTC, data security needs should be considered in all business decision-making. FTC publications have  
21 repeatedly and emphatically discussed the importance of reasonable data security protocols, systems,  
22 and procedures. For example, in 2023, the FTC released *Start with Security: A Guide for Business*  
23 *(Lessons Learned from FTC Cases)*. In this guidance, the FTC advised businesses to, among other  
24 things:  
25

- 26 (1) "Hold on to information only as long as you have a legitimate business need;"  
27 (2) "Restrict access to sensitive data;"  
28

(3) “Limit administrative access;”

(4) “Use industry-tested and accepted methods [for data security];”

(5) “Continuously validate access to data;” and

(6) “Monitor activity on your network.”<sup>18</sup>

43. The FTC also encourages businesses to take other protective measures, including, but not limited to, ensuring and verifying that any third-parties with access to sensitive data or information are using reasonable data security procedures, technologies, and protocols, and requiring enhanced or strong passwords for access to sensitive data or information.

44. The FTC has a record of bringing enforcement cases against businesses that failed to adequately and reasonably protect and store sensitive data. Such failures constitute an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015).

45. States throughout the country also have data security laws requiring businesses that own, maintain, or license PII or PHI to protect PHI and PII from unauthorized access and to implement and employ reasonable data security policies, procedures, and practices.

46. Based upon the known details of the Data Breach and how it occurred, ETS failed to fully comply with industry-standard cybersecurity measures and practices, including, but not limited to, authentication safeguards; intrusion monitoring, prevention, and detection; secure credential storage and creation; user-activity monitoring; data-loss prevention; access restrictions and monitoring; proper firewall configurations and network segmentation; limited data retention periods; and rate limiting.

---

<sup>18</sup> FTC, *Start with Security: A Guide for Business (Lessons Learned from FTC Cases)*, <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know> (last visited Oct. 18, 2026).

## V. CLASS ALLEGATIONS

47. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Rule 23 of the Federal Rule of Civil Procedure. The Classes that Plaintiffs seek to represent are as follows:

**Nationwide Class:** All natural persons whose Personally Identifiable Information or Protected Health Information was compromised as a result of the Data Breach.

**California Subclass:** All natural persons in California whose Personally Identifiable Information or Protected Health Information was compromised as a result of the Data Breach.

Collectively, the Class and Subclasses are referred to as the “Classes” or “Class Members.”

48. Excluded from the Classes are Defendant, any entity in which the Defendant has a controlling interest, any of the officers or directors of Defendant, the legal representatives, heirs, successors, and assigns of Defendant, and any Judge to whom this case is assigned, and his or her immediate family.

49. The definition of the Class may be further modified or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court. Plaintiffs expressly reserve the right to amend or modify the definitions of the proposed Classes before the Court determines whether certification is appropriate.

50. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or the identity of the Class Members because such information is in the exclusive control of Defendant. Nevertheless, based on published reports, the Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

1 The names, phone numbers, and addresses of Class Members are identifiable through documents  
2 maintained by Defendant.

3 51. **Commonality and Predominance:** This action involves common questions of law and  
4 fact as to all Class Members, which predominate over any question solely affecting individual Class  
5 Members. Common questions of law and fact include, but are not limited to, the following:

- 6 (1) Whether ETS engaged in the conduct alleged herein;
- 7 (2) Whether Plaintiffs and the Class are entitled to damages and equitable relief due  
8 to ETS' conduct.
- 9 (3) Whether ETS had a legal duty to use reasonable security measures to protect  
10 Plaintiffs and Class Members' PII and PHI;
- 11 (4) Whether ETS' failure to implement effective security measures to protect Class  
12 Members' PII and PHI was negligent;
- 13 (5) Whether Plaintiffs and Class Members are entitled to injunctive relief; and  
14 (6) Whether Plaintiffs and Class Members are entitled to declaratory relief.

15 52. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because all  
16 Class Members were comparably injured through ETS' substantially uniform misconduct described  
17 above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other  
18 members of the Class that they seek to represent, and there are no defenses that are unique to Plaintiffs.  
19 Plaintiffs and Class Members' claims and injuries arise from the same facts and are based on the same  
20 law.  
21

22 53. **Adequacy:** Plaintiffs are adequate Class Representatives because their interests do not  
23 conflict with the interests of other Class Members they seek to represent; Plaintiffs have retained  
24 competent counsel that are experienced in complex class action litigation; and Plaintiffs intend to  
25 vigorously prosecute this action. The interests of Class Members will be fairly and adequately protected  
26 by Plaintiffs and their counsel.  
27  
28

54. **Superiority:** A class action is superior to other available methods for fair and efficient adjudication of this controversy. No unusual difficulties are likely to be encountered in the management of this class action. The damages suffered by Class Members are relatively small compared to the expense required to individually litigate their claims against ETS, so, absent class-wide adjudication, it would be virtually impossible for Class Members to seek individual redress against ETS' wrongful conduct.

## VI. CAUSES OF ACTION

### COUNT ONE

#### NEGLIGENCE

55. Plaintiffs incorporate paragraphs 1 through 54 above, as if fully set forth herein.

56. Plaintiffs bring this Count individually and on behalf of the Nationwide Class and California Subclass.

57. As part of its business, ETS solicited, collected, and maintained Plaintiffs and Class Members' PII and PHI.

58. ETS' business depended upon collecting Plaintiffs and Class Members' PII and PHI because services it provides requires that it use Plaintiffs and Class Members' PII and PHI.

59. ETS owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risks of harm to Plaintiffs and Class Members collecting, employing, maintaining, storing, and managing PII or PHI.

60. Upon collecting, accepting custody of, and storing Plaintiffs and Class Members' PII and PHI, ETS undertook and owed a duty to Plaintiffs and Class Members to secure protect their PHI and PII using proven, effective, reliable and safe means and methods.

61. ETS' duties to Plaintiffs and Class Members extended to protecting them from the foreseeable risk of third parties' criminal conduct. Defendant owed a duty of care to Plaintiffs and Class

1 members whose PII and PHI was entrusted to it. ETS' duties included, but were not limited to, the  
 2 following:

- 3 (1) taking reasonable care in obtaining, securing, retaining, safeguarding, and  
 4 deleting PII and PHI in its possession;
- 5 (2) protecting PHI and PII using reasonable and adequate security procedures and  
 6 systems consistent and compliant with industry standards;
- 7 (3) having procedures in place to prevent the loss or unauthorized dissemination of  
 8 PHI or PII in its possession;
- 9 (4) employing reasonable and adequate security measures and otherwise  
 10 safeguarding and protecting the PII and PHI of Plaintiffs and Class Members  
 11 pursuant to federal and state regulations, including, but not limited to the FTCA;
- 12 (5) implementing processes to expeditiously detect a data breach and acting timely  
 13 on indicators of compromise or warnings or signs of a data breach; and
- 14 (6) promptly notifying Plaintiffs and Class members of the breach, and precisely  
 15 disclosing the type(s) of information compromised and their scope.

16  
 17  
 18 62. Only ETS was able to secure its own programs and systems and ensure that the security  
 19 measures it used were sufficient to protect the PII and PHI of Plaintiffs and Class Members.

20 63. ETS breached its duty of care because it failed to adequately protect and safeguard the  
 21 PII and PHI belonging to Plaintiffs and Class Members. ETS' breaches included, but were not limited  
 22 to:

- 23 (1) Failing to use adequate and reasonable security systems and policies for  
 24 safeguarding the PII and PHI it possessed;
- 25 (2) Failing to ensure that it did not maintain or keep PII or PHI on its systems, servers,  
 26 and devices for longer than necessary;

- (3) Failing to use reasonable care in protecting, maintaining, using, and erasing the PII and PHI that it possessed.
- (4) Failing to adequately train and test its employees on sufficiently and safely sending and storing PII and PHI;
- (5) Failing to enforce security policies for protecting Plaintiffs and Class Members' PII and PHI;
- (6) Failing to reasonably implement protocols for promptly detecting security incidents, data breaches, or unauthorized access to sensitive data, including Plaintiffs and Class Members' PII and PHI;
- (7) Failing to train employees to avoid phishing emails and test employees' conduct upon receipt of suspicious emails;
- (8) Failing to use reasonable and adequate industry standard security systems and devices for emails, including SPAM filters, DMARC compliance, and/or Sender Policy Framework compliance.

64. ETS was fully aware that Plaintiffs and Class Members' PII was sensitive, that Plaintiffs and Class Members would suffer significant and varied injuries if their PII or PHI was wrongfully disclosed or exfiltrated, and that providing reasonable and sufficient security for Plaintiffs and Class Members' PII and PHI was substantially important.

65. Plaintiffs and Class Members were foreseeable victims of any insufficient security protocols and practices by ETS. Defendant had a duty of care to not subject Plaintiffs and Class Members to an unreasonable risk of injury. Defendant knew that cybercriminals frequently use cyberattacks to steal sensitive PII and PHI for their own gain and in doing so, cause serious harm to those persons to whom the PHI and PII pertains.

1           66. Plaintiffs and Class Members' PII and PHI have been publicly exposed as a direct result  
2 of ETS' breach of its duty to use reasonable care to adequately protect and secure Plaintiffs and Class  
3 Members' PII and PHI.

4           67. Despite knowing its networks, systems, protocols, policies, procedures, and practices, as  
5 described above, were not adequately designed, implemented, maintained, monitored, and tested to  
6 ensure that Plaintiffs and Class Members' PII and PHI were secured from unauthorized access, ETS  
7 ignored the inadequacies and were oblivious to the risk of unauthorized access they had created.

8           68. ETS' wrongful acts and omissions constituted and continue to constitute common law  
9 negligence. And because ETS' behavior establishes facts evidencing a reckless disregard for Plaintiffs  
10 and Class Members' rights, ETS was grossly negligent.

11           69. ETS' conduct also constitutes negligence per se. The FTC Act prohibits "unfair practices  
12 in or affecting commerce."<sup>19</sup> It imposed and continues to impose on ETS a duty to Plaintiffs and Class  
13 Members to provide adequate and fair practices, computer systems, and data security for safeguarding  
14 Plaintiffs and Class Members' PII and PHI. In enforcement actions, the FTC has treated businesses'  
15 failure to employ reasonable measures to adequately secure consumer's confidential data as an unfair  
16 act or practice prohibited by Section 5 of the FTC Act.<sup>20</sup> ETS' failures to use reasonable and appropriate  
17 methods to guard Plaintiffs and Class Members' PII and PHI against unauthorized access is an unfair  
18 act or practice that Section 5 of the FTC Act prohibits. ETS violated the FTC Act by failing to comply  
19 with industry-standard data security practices, as described above. ETS' collection and maintenance of  
20  
21  
22

23  
24 \_\_\_\_\_  
<sup>19</sup> 15 U.S.C. § 45(a).

25 <sup>20</sup> See, e.g., Complaint, *Drizly, LLC and James Cory Rellas*, FTC Matter No. 2023185 (Oct. 24, 2022),  
26 [https://www.ftc.gov/system/files/ftc\\_gov/pdf/202-3185-Drizly-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf) (last visited Oct. 18,  
27 2026); Complaint, *Fandango*, FTC Matter No. 1323089 (Aug. 19 2014),  
28 <https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf> (last visited Oct. 18,  
2026).

1 Plaintiffs and Class Members' PII and PHI were actions central to its business and affected commerce.  
2 The class of people that the FTC Act is intended to protect include Plaintiffs and Class Members.

3 70. ETS also engaged in unlawful, unfair and fraudulent practices within the meaning, and  
4 in violation of, the California Unfair Competition Law by virtue of the above-described wrongful  
5 actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data  
6 breach. In the course of conducting its business, ETS committed "unlawful" business practices by, *inter*  
7 *alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit  
8 appropriate data security processes, controls, policies, procedures, protocols, and software and hardware  
9 systems to safeguard and protect Plaintiffs and California Subclass members' PII and PHI, and by  
10 violating the statutory and common law alleged herein.

11 71. ETS' above-described wrongful actions, inaction, omissions, want of ordinary care,  
12 misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in  
13 violation of the UCL in that ETS' wrongful conduct is substantially injurious to consumers, offends  
14 legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. ETS'  
15 practices are also contrary to legislatively declared and public policies that seek to protect PII and PHI  
16 and ensure that entities who solicit or are entrusted with PII or PHI utilize appropriate security measures,  
17 as reflected by laws such as the Article I, Section 1 of the California Constitution (California's  
18 constitutional right to privacy) and the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45).  
19 The gravity of ETS' wrongful conduct outweighs any alleged benefits attributable to such conduct.  
20 There were reasonably available alternatives to further ETS' legitimate business interests other than  
21 engaging in the above-described wrongful conduct.  
22

23 72. As a direct and proximate result of ETS' above-described wrongful actions, inaction,  
24 omissions, and want of ordinary care that directly and proximately caused the data breach and its  
25 violations of the UCL, Plaintiffs and California Subclass Members have suffered (and will continue to  
26 suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent,  
27  
28

1 immediate and the continuing increased risk of identity theft and identity fraud – risks justifying  
2 expenditures for protective and remedial services for which they are entitled to compensation, (ii)  
3 invasion of privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages, (v)  
4 deprivation of the value of their PII and PHI, for which there is a well-established national and  
5 international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring  
6 financial accounts, and mitigating damages.

7  
8 73. ETS' negligence is directly linked to Plaintiffs and Class Members' injuries. As a result  
9 of ETS' reckless disregard for Plaintiffs and Class Members' rights by failing to secure their PII and  
10 PHI, despite knowing its networks, systems, protocols, policies, procedures, and practices were not  
11 adequately designed, implemented, maintained, monitored, and tested, Plaintiffs and Class Members  
12 suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud,  
13 identity theft, financial and other harm, and continue to be at imminent risk of additional injuries as a  
14 foreseeable and proximate result of ETS' negligence. Plaintiffs and Class Members must monitor their  
15 financial accounts and credit histories more closely and frequently to guard against identity theft.  
16 Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-  
17 of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other  
18 protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class  
19 Members' PII and PHI has also diminished the value of their PHI.  
20

21 74. Plaintiffs and Class Members are accordingly entitled to damages in an amount to be  
22 proven at trial.  
23

## 24 **COUNT TWO**

### 25 **BREACH OF THIRD-PARTY BENEFICIARY AGREEMENTS**

26 75. Plaintiffs restate the allegations in Paragraphs 1 through 54 above, as if fully set forth  
27 herein.  
28

1           76. Plaintiffs bring this Count individually and on behalf of the Nationwide Class and  
2 California Subclass.

3           77. Upon information and belief, ETS entered into valid contracts with the state of California  
4 and political divisions or subdivisions thereof, including, but not limited to, the California Department  
5 of Education and California school districts or municipalities pursuant to which ETS was required to  
6 engage in and carry out data security practices, procedures, and protocols sufficient to safeguard the PII  
7 and PHI of Plaintiffs and Class Members that ETS required to provide its services.

8           78. These contractual agreements were made expressly for the benefit of Plaintiffs and Class  
9 Members, as it was their PII and PHI that Defendants agreed to receive and protect.  
10

11           79. The benefit of collecting and protecting the PII and PHI of Plaintiffs and Class Members  
12 was the direct and primary objective of the contracting parties. Plaintiffs and Class Members were direct,  
13 intended, and express beneficiaries of these agreements.

14           80. Plaintiffs and Class Members are also intended third-party beneficiaries of these  
15 agreements because recognizing them as such is appropriate to effectuate the parties' intentions, and the  
16 circumstances indicate that Defendant intended to give the beneficiaries the benefit of the promised  
17 performance.  
18

19           81. Defendant knew that, if it breached these agreements, it would harm Californians,  
20 including Plaintiffs and the Class. Defendant knew that the harms would include fraudulent transactions  
21 and the victims' need to expend time and money to protect themselves from identity theft.

22           82. Defendant breached its contracts when it failed to use adequate and reasonable data  
23 security protocols, procedures, measures, and technologies and, in so failing, allowed the data breach to  
24 transpire.  
25

26           83. Defendant's failure to use reasonable data security protections accordingly injured  
27 Plaintiffs and Class Members. Plaintiffs and Class Members are entitled to damages in an amount to be  
28 determined at trial as well as costs and attorneys' fees incurred.

**COUNT THREE**

**BREACH OF IMPLIED CONTRACTS**

84. Plaintiffs incorporate paragraphs 1 through 54 above, as though fully set forth herein.

85. Plaintiffs bring this Count individually and on behalf of the Nationwide Class and California Subclass.

86. Plaintiffs and Class Members provided their PII and PHI to ETS to obtain ETS' services.

87. By providing their PII and PHI, and upon ETS' acceptance of such information, Plaintiffs and Class Members on one hand, and ETS on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the services provided, whereby ETS was obligated to take reasonable steps to secure and safeguard that information.

88. ETS had an implied duty of good faith to ensure that the PII and PHI of Plaintiffs and Class Members in its possession was only used in accordance with its contractual obligations.

89. ETS was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs and Class Members' PII and PHI and to comply with industry standards and state laws and regulations for the security of this information, and ETS expressly assented to these terms in its Privacy Policies.

90. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to ETS, including paying for the services provided by ETS and/or providing the PII and PHI required by ETS.

91. ETS breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs and Class Members' PII and PHI, resulting in the Data Breach. ETS unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members.

92. Further, on information and belief, ETS has not yet provided data breach notifications to some affected Class Members who may already be victims of identity fraud or theft, or are at imminent

1 risk of becoming victims of identity theft or fraud, associated with the PII and PHI that they provided to  
2 ETS. These Class Members are unaware of the potential source for the compromise of their PII and PHI.

3 93. The data breach was a reasonably foreseeable consequence of ETS' actions in breach of  
4 these contracts.

5 94. As a result of ETS' conduct, Plaintiffs and Class Members did not receive the full benefit  
6 of the bargain, and instead received services that were of a diminished value as compared to the secure  
7 services they paid for. Plaintiffs and Class Members, therefore, were damaged in an amount at least  
8 equal to the difference in the value of the secure services they paid for and the services they received.  
9

10 95. Neither Plaintiffs, nor Class Members, nor any reasonable person would have provided  
11 their PII or PHI to ETS, or consented to the provisioning of their PII or PHI to ETS, had ETS disclosed  
12 that its security was inadequate or that it did not adhere to industry-standard security measures.

13 96. As a result of ETS' breach, Plaintiffs and Class Members have suffered actual damages  
14 resulting from theft of their PII and PHI, as well as the loss of control of their PII and PHI, and remain  
15 at imminent risk of suffering additional damages in the future.  
16

17 97. As a result of ETS' breach, Plaintiffs and Class Members have suffered actual damages  
18 resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent data  
19 breach, including, but not limited to, taking steps to protect themselves from the loss of their PII and  
20 PHI. As a result, Plaintiffs and Class Members have suffered actual identity theft and the inability to  
21 control their PII and PHI.

22 98. Accordingly, Plaintiffs and Class Members have been injured as a result of ETS' breach  
23 of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.  
24

#### 25 **COUNT FOUR**

#### 26 **BREACH OF FIDUCIARY DUTY**

27 99. Plaintiffs incorporate paragraphs 1 through 54 above, as though fully set forth herein.  
28

1           100. ETS formed a special relationship with Plaintiffs and Class Members when it collected,  
2 processed and maintained Plaintiffs and Class Members' highly sensitive data and in doing so, took on  
3 the responsibilities and obligations of safeguarding and protecting that data. ETS was a fiduciary as to  
4 Plaintiffs and Class Members because it contracted with California to collect, process and maintain their  
5 data and accepted custody of their data in confidence.

6           101. Only ETS could ensure that it adequately and reasonably protected Plaintiffs and Class  
7 Members data. Plaintiffs and Class Members could not safeguard the information for ETS once it was  
8 within ETS' custody. ETS, not Plaintiffs and Class Members, exercised control and had dominion over  
9 the data systems, technologies, protocols, and procedures that ETS used to collect, process and maintain  
10 Plaintiffs and Class Members' data.

11           102. Accordingly, ETS had a fiduciary duty to Plaintiffs and Class Members to act for their  
12 benefit as to matters within the scope of ETS' relationship with Plaintiffs and Class Members. The scope  
13 of that relationship included the protection and safeguarding of Plaintiffs and Class Members' data.  
14

15           103. ETS violated its fiduciary duty because it failed to take reasonable and adequate measures  
16 to protect Plaintiffs and Class Members' data.  
17

18           104. As a proximate and direct consequence of ETS's violation of its fiduciary duty to  
19 Plaintiffs and Class Members, Plaintiffs and Class Members experienced, and will continue to  
20 experience, the injuries described in paragraphs 1 through 54 of this Complaint and are entitled to  
21 compensatory and consequential damages in an amount to be established at trial.  
22

## 23                                   **COUNT FIVE**

### 24                                   **UNJUST ENRICHMENT**

25           105. Plaintiffs incorporate paragraphs 1 through 54 above, as though fully set forth herein.

26           106. Plaintiffs bring this Count individually and on behalf of the Nationwide Class and  
27 California Subclass.  
28

1           107. Plaintiffs and Class Members conferred a monetary benefit on ETS in the form of  
2 monetary payments—directly or indirectly—for testing services and accommodations determinations.

3           108. ETS collected, maintained, and stored the PII and PHI of Plaintiffs and Class Members  
4 and, as such, ETS had knowledge of the monetary benefits conferred by Plaintiffs and Class Members.  
5 The collection, maintenance, and storage of Plaintiffs and Class Members’ PII and PHI was a central  
6 part of ETS’ business and ability to gain compensation for its services.

7           109. The money that ETS directly or indirectly received from Plaintiffs and Class Members  
8 should have been used to pay, at least in part, for the administrative costs and implementation of data  
9 management and security. ETS failed to implement—or adequately implement—practices, procedures,  
10 and programs to secure sensitive PII and PHI, as evidenced by the data breach.

11           110. As a result of ETS’ failure to implement security practices, procedures, and programs to  
12 secure sensitive PII and PHI, Plaintiffs and Class Members suffered actual damages in an amount equal  
13 to the difference in the value between services with reasonable data privacy that Plaintiffs and Class  
14 Members paid for, and the services they received without reasonable data privacy.  
15

16           111. Under principles of equity and good conscience, ETS should not be permitted to retain  
17 money belonging to Plaintiffs and Class Members because ETS failed to implement the data  
18 management and security measures that are mandated by industry standards and that Plaintiffs and Class  
19 Members paid for, either directly or indirectly.  
20

21           112. ETS should be compelled to disgorge into a common fund for the benefit of Plaintiffs  
22 and the Class all unlawful or inequitable proceeds received by ETS. A constructive trust should be  
23 imposed upon all unlawful and inequitable sums received by ETS traceable to Plaintiffs and Class  
24 Members.  
25  
26  
27  
28

**COUNT SIX****CALIFORNIA UNFAIR COMPETITION LAW  
Cal. Bus. & Prof. Code §§ 17200, *et seq.* (“UCL”)**

113. Plaintiffs, individually and on behalf of the California Subclass, incorporate paragraphs 1 through 54 above, as though fully set forth herein.

114. The UCL prohibits any “unlawful,” “fraudulent” or “unfair” business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, ETS engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

115. In the course of conducting its business, ETS committed “unlawful” business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs and California Subclass Members’ PII and PHI, and by violating the statutory and common law alleged herein. Plaintiffs and California Subclass Members reserve the right to allege other violations of law by ETS constituting other unlawful business acts or practices. ETS’ above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

116. ETS’ above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute “unfair” business acts and practices in violation of the UCL in that ETS’ wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. ETS’ practices are also contrary to legislatively declared and public policies that seek to protect PII and PHI and ensure that entities who solicit or are entrusted with PII or PHI utilize appropriate security measures, as reflected by laws such as the Article I, Section 1 of the California Constitution (California’s

1 constitutional right to privacy) and the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. § 45).  
2 The gravity of ETS’ wrongful conduct outweighs any alleged benefits attributable to such conduct.  
3 There were reasonably available alternatives to further ETS’ legitimate business interests other than  
4 engaging in the above-described wrongful conduct.

5 117. As a direct and proximate result of ETS’ above-described wrongful actions, inaction,  
6 omissions, and want of ordinary care that directly and proximately caused the data breach and its  
7 violations of the UCL, Plaintiffs and California Subclass Members have suffered (and will continue to  
8 suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent,  
9 immediate and the continuing increased risk of identity theft and identity fraud – risks justifying  
10 expenditures for protective and remedial services for which they are entitled to compensation, (ii)  
11 invasion of privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages, (v)  
12 deprivation of the value of their PII and PHI, for which there is a well-established national and  
13 international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring  
14 financial accounts, and mitigating damages.  
15

16 118. Unless restrained and enjoined, ETS will continue to engage in the above-described  
17 wrongful conduct and more data breaches will transpire. Plaintiffs, therefore, individually, and on behalf  
18 of California Subclass Members, and the general public, also seek restitution and an injunction  
19 prohibiting ETS from continuing such wrongful conduct, and requiring ETS to modify its corporate  
20 culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate  
21 data security processes, controls, policies, procedures protocols, and software and hardware systems to  
22 safeguard and protect the PII and PHI entrusted to it, as well as all other relief the Court deems  
23 appropriate, consistent with Bus. & Prof. Code § 17203.  
24  
25  
26  
27  
28

**COUNT SEVEN**

**INVASION OF PRIVACY  
Cal. Const. art. I, § 1**

119. Plaintiffs, individually and on behalf of the California Subclass, incorporate paragraphs 1 through 54 above, as though fully set forth herein.

120. Article I, section 1 of the California Constitution provides that all people have inalienable rights, among which is the right of privacy. The California Constitution guarantees a privacy right enforceable against private entities.

121. Plaintiffs and California Subclass members have a privacy interest in the data that ETS wrongfully failed to protect. Their privacy interest in that data is substantial and legally protected. Plaintiffs and California Subclass Members also had a reasonable expectation of privacy in that data, which they provided, or had provided on their behalf and for their benefit. Plaintiffs and California Subclass Members reasonably expected that ETS would safeguard the data to which ETS had been entrusted. Plaintiffs and California Subclass Members never provided ETS with any consent to the disclosure of the data in question to unauthorized third parties.

122. ETS has engaged in serious invasion of the privacy rights of Plaintiffs and California Subclass Members. ETS failed to detect a prolonged breach of their systems after failing to maintain adequate and reasonable data security measures in the first place. ETS's failures constitute an egregious breach of social norms and is offensive.

123. As a proximate and direct consequence of ETS's gross invasion of their privacy and privacy rights, Plaintiffs and California Subclass Members have suffered substantial injuries, including loss of privacy, emotional distress, and the other harms described herein. Plaintiffs and California Subclass Members are accordingly entitled to damages and equitable relief.

**COUNT EIGHT**

**DECLARATORY JUDGMENT**

124. Plaintiffs incorporate all paragraphs above, as though fully set forth herein.

125. Plaintiffs bring this Count individually and on behalf of the Nationwide Class and California Subclass.

126. Plaintiffs and Class Members have stated claims against Defendant based on negligence, breach of third-party beneficiary agreements, breach of implied contracts, breach of fiduciary duty, unjust enrichment, invasion of privacy, and violation of the California Unfair Competition Law.

127. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII and PHI of Plaintiffs and Class Members, as evidenced by the data breach.

128. As a result of the data breach, ETS' systems are more vulnerable to unauthorized access and require more stringent measures to be taken to safeguard the PII and PHI of Plaintiffs and Class Members going forward.

129. Plaintiffs seek a declaration that ETS must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII and PHI of Plaintiffs and Class Members. Specifically, Plaintiffs and Class Members seek a declaration that ETS' existing security measures do not comply with their obligations, and that ETS must implement and maintain reasonable security measures on behalf of Plaintiffs and Class Members to comply with their data security obligations.

**VII. PRAYER FOR RELIEF**

130. Plaintiffs, individually and on behalf of the proposed Classes, request that the Court:

(1) Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' Counsel as Class Counsel for Plaintiffs to represent the Class.

(2) Find that Defendants breached their duties to safeguard and protect the PII and

PHI of Plaintiffs and Class Members that was compromised in the data breach;

- (3) Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution and disgorgement;
- (4) Award equitable, injunctive and declaratory relief as may be appropriate;
- (5) Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;
- (6) Award pre-judgment and post-judgment interest as prescribed by law; and
- (7) Grant additional legal or equitable relief as the Court may find just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: October 20, 2026

Respectfully submitted,

**COTCHETT, PITRE & McCARTHY, LLP**

/s/ Kelly A. Aristides

Kelly A. Aristides (SBN 357856)  
Karin Swope (pro hac vice forthcoming)  
Andrew J. Fuller (pro hac vice forthcoming)  
1809 7th Avenue, Suite 1610  
Seattle, WA 98101  
Telephone: (206) 802-1272  
Facsimile: (206) 299-4184  
kswope@cpmlegal.com  
afuller@cpmlegal.com  
karistides@cpmlegal.com

Joseph W. Cotchett (SBN 36324)  
Zachary Zaharoff (SBN 321878)  
840 Malcolm Rd.  
Burlingame, CA 94010  
Telephone: (650) 697-6000  
jcotchett@cpmlegal.com

*Attorneys for Plaintiffs and the Proposed Class*