UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

TIAA POINTER, individually and on behalf of all others similarly situated, Plaintiff, v. THE UNIVERSITY OF PHOENIX, INC., PHOENIX EDUCATION PARTNERS, INC., and ORACLE CORPORATION, Defendants.	Case No. 1:26-cv-00009 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Tiaa Pointer ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendants The University of Phoenix, Inc., Phoenix Education Partners, Inc. (together "UOPX") and Oracle Corporation ("Oracle" and with UOPX, "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard approximately 3,489,274 individuals' (including Plaintiff's) personally identifying information ("PII") including names, dates of birth, Social Security numbers, and bank account and routing numbers.

2. The University of Phoenix, Inc. is a private, for-profit university, and is a subsidiary of Phoenix Education Partners, Inc. Oracle is a technology company offering a variety of products

and services for businesses, including its E-Business Suite software ("EBS"). UOPX contracts with Oracle to use its EBS.

3. Between approximately August 13 and August 22, 2025, an unauthorized third party exploited a vulnerability in Oracle's EBS software to gain access to Oracle's network systems and acquire files containing the PII of Oracle's clients' customers, including Plaintiff and Class members (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to, or sharing PII with third parties that failed to, implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class members' PII from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII was exposed as a result of the Data Breach, which occurred between approximately August 13 and August 22, 2025.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of implied contract, unjust enrichment, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Tiaa Pointer

7. Plaintiff is a citizen and resident of Illinois.

8. Plaintiff is a former student of the University of Phoenix. As a condition of providing education services to Plaintiff, UOPX required her to provide it with her PII, including the PII accessed and stolen by cybercriminals in the Data Breach. UOPX in turn shared this information with Oracle in connection with utilizing Oracle's EBS software.

9. At all relevant times, Defendants stored and maintained Plaintiff's PII on their network systems, including the systems impacted in the Data Breach.

10. Plaintiff received a notice letter from UOPX notifying her that her PII, including her name and Social Security number, was accessed and acquired by an unauthorized third party in the Data Breach.

11. Since the Data Breach, Plaintiff has experienced hard inquiries on her credit that she was not responsible for.

12. As a result of the Data Breach, Plaintiff experienced a large increase in the number of spam calls, texts, and emails she receives, including emails regarding loan applications she is unfamiliar with.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; time and effort lost attempting to mitigate the harm caused by the Data Breach; and deprivation of the value of her PII.

Defendant The University of Phoenix, Inc.

14. Defendant The University of Phoenix, Inc. is an Arizona corporation with its principal place of business located at 4035 South Riverpoint Parkway, Phoenix, AZ 85040. It may be served through its registered agent: Corporation Service Company, located at 7955 South Priest Dr., Suite 102, Tempe, AZ 85284.

Defendant Phoenix Education Partners, Inc.

15. Defendant Phoenix Education Partners, Inc. is a Delaware corporation with its principal place of business located at 4035 South Riverpoint Parkway, Phoenix, AZ 85040. It may be served through its registered agent: Corporation Service Company, located at 251 Little Falls Drive, Wilmington, DE 19808.

Defendant Oracle Corporation

16. Defendant Oracle Corporation is a Delaware corporation with its principal place of business located at 2300 Oracle Way, Austin, TX 78741. It may be served through its registered agent: Corporation Service Company, located at 211 E. 7th Street, Suite 620, Austin, TX 78701.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

18. This Court has general personal jurisdiction over Defendant Oracle Corporation because it transacts business within this State and maintains its principal place of business in this District. This Court has personal jurisdiction over Defendants The University of Phoenix, Inc. and

Phoenix Education Partners, Inc. because they contract for business in this State and contract for goods or services in this State.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Oracle Corporation's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

20. The University of Phoenix is an online university designed for working adults.[1] Phoenix Education Partners, Inc. is the parent company of The University of Phoenix, Inc.[2] Oracle "provides products and services that address enterprise information technology (IT) needs."[3]

21. In the regular course of its business, UOPX collects and maintains the PII of its current and former students, including the PII stolen in the Data Breach, before providing them with education services. UOPX in turn shares this PII with Oracle in connection with receiving services from Oracle.

22. On its website, UOPX maintains a Privacy Policy (the "Privacy Policy") which describes its practices regarding the PII it collects.[4] In the Privacy Policy, UOPX claims it "recognizes the importance of privacy."[5]

---

[1] *Who we are*, UNIV. PHX., https://www.phoenix.edu/about.html (last accessed Jan. 2, 2026).
[2] *Overview*, PHX. EDUC. PARTNERS, https://phoenixeducationpartners.com/overview/default.aspx (last accessed Jan. 2, 2026).
[3] Oracle, *Annual Report (Form 10-K)* (June 18, 2025), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001341439/7455eba6-bb80-41d3-96b7-12111eae648c.pdf [hereinafter, "Oracle *Form 10-K*"].
[4] *University of Phoenix Privacy Policy*, UNIV. PHX. (Aug. 3, 2025), available at: https://web.archive.org/web/20250909095310/https://www.phoenix.edu/copyright-legal/privacy-policy.html.
[5] *Id.*

23. UOPX's Privacy Policy lists when UOPX may disclose the PII it collects and stores, including to third-party service providers.[6] UOPX claims to have "implemented security measures to protect against the loss, misuse, and alteration of the" PII it collects.[7]

24. UOPX is aware of the risk of a data breach or unauthorized release of PII, as evidenced by including a data breach as a risk factor in its 2025 Form 10-K.[8] UOPX admits "[i]f we fail to effectively assess and identify cybersecurity risks associated with the use of technology in our business operations, we may become increasingly vulnerable to such risks."[9] UOPX also claims to "vet the capabilities of current and future" IT vendors.[10]

25. UOPX acknowledges its "collection, use, retention, and other processing of personal information—both in our capacity as a data controller as well as a data processor in our role as a service provider—makes us and the systems or vendors we rely upon a target for cyber-attacks."[11] UOPX further acknowledges that much of the PII it collects "is held and managed by third-party vendors, and as a result, [it is] . . . susceptible to operational and information security risks resulting from system failures and cybersecurity incidents of [its] third-party vendors, and the technology and services they rely on to provide services to [it]."[12]

26. UOPX admits the PII it collects and shares is "generally higher risk and/or sensitive, which comes with higher regulatory scrutiny and makes [it] a bigger target for malicious

---

[6] *Id.*
[7] *Id.*
[8] Phoenix Education Partners, *Annual Report (Form 10-K)* (Nov. 20, 2025), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001600222/70e4abe0-3309-463d-aa50-3ba19bc76626.pdf [hereinafter, "UOPX *Form 10-K*"].
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

cyber threats."[13] It further admits, "[o]ur size and the amount and sensitivity of personal data that we collect or otherwise process makes us a prominent target for cyber-attacks within the education industry."[14]

27. UOPX asserts it "maintain[s] a vendor management process to review the security measures undertaken by [its] vendors to help try and manage" cybersecurity risks.[15]

28. Oracle similarly admits it "is a target for computer hackers, cyber threats and other bad actors because our products and services store, retrieve, process and manage large amounts of data, including sensitive data."[16] It also admits it is "regularly subject to attempts by third parties to identify and exploit product and service vulnerabilities, penetrate or bypass our security measures and gain unauthorized access to our or our customers', partners' and suppliers' software, hardware and cloud offerings, networks and systems."[17]

29. Oracle claims to "leverage industry standard security frameworks to evaluate our security controls."[18] It also claims to "employ various monitoring tools to track suspicious or anomalous activity across our networks, systems, and data, and we simulate cyber threats to proactively address vulnerabilities."[19] Oracle further claims to "undergo security-related industry certifications and attestations by external auditors, including System and Organization Controls (SOC) 1, SOC 2, International Organization for Standardization (ISO) 27001, 27017 and 27018,

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] Oracle *Form 10-K*, *supra* note 3.
[17] *Id.*
[18] *Id.*
[19] *Id.*

Cloud Security Alliance Security Trust Assurance and Risk (CSA STAR), Payment Card Industry Data Security Standard (PCI DSS) and other compliance frameworks."[20]

30. Oracle maintains a Service Privacy Policy (the "OSPP") that "describes the privacy and security practices that Oracle Corporation and its affiliates ('Oracle') employ when handling" PII "for the provision of Technical Support, Consulting, Cloud or other services, including those provided via mobile application, (the 'Services') provided to Oracle customers."[21]

31. In its OSPP, Oracle promises it "has implemented and will maintain technical and organizational measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to" PII.[22]

32. Oracle represents it will provide notification of a data breach "without undue delay."[23] Oracle promises it "does not share or sell [PII] subject to this Privacy Policy with third parties for any commercial purposes."[24]

33. Oracle claims it "has implemented appropriate technical, physical and organizational measures in accordance with the Oracle Corporate Security Practices designed to protect personal information against . . . unauthorized disclosure or access."[25]

34. Oracle promises it "continually works to strengthen and improve the security controls and practices for Oracle internal operations and services offered to customers."[26]

---

[20] *Id.*
[21] *Oracle Services Privacy Policy*, ORACLE (Aug. 19, 2025), https://www.oracle.com/legal/privacy/services-privacy-policy/ (last accessed Jan. 2, 2026) [hereinafter, "*OSPP*"].
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Oracle Corporate Security Practices, Oracle, https://www.oracle.com/contracts/docs/corporate-security-practices-4490843.pdf (last accessed Jan. 2, 2026).

35. Plaintiff and Class members are, or were, customers of Oracle's clients, and Oracle stored Plaintiff's and Class members' PII on its network systems.

The Data Breach

36. Between approximately August 13 and August 22, 2025, "an unauthorized third-party exploited a previously unknown software vulnerability in Oracle EBS to exfiltrate certain data from within the University of Phoenix's Oracle EBS environment."[27] UOPX admits the cybercriminals accessed and exfiltrated information including names, dates of birth, Social Security numbers, and bank account and routing numbers.[28]

37. Despite learning of the Data Breach on or about November 21, 2025, UOPX waited until approximately December 21, 2025—a month later—to announce the Data Breach and begin notifying Plaintiff and Class members that their PII was accessed and acquired by unauthorized persons.[29]

38. Oracle's investigation revealed a vulnerability in its EBS software known as "CVE-2025-61882."[30] This vulnerability was "remotely exploitable without authentication" and could be "exploited over a network without the need for a username and password."[31] If exploited, the vulnerability could allow cybercriminals to remotely execute code in Oracle's EBS software system.[32]

---

[27] University of Phoenix, Inc., *Data Breach Notification*, ME. ATT'Y GEN. (Dec. 21, 2025), available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/422db005-448f-4772-afc6-07dabfa169a8.html.
[28] *University of Phoenix Media Center*, UNIV. PHX., https://www.phoenix.edu/media-center.html (last accessed Jan. 2, 2026).
[29] *See Data Breach Notification*, *supra* note 27.
[30] *Oracle Security Alert Advisory - CVE-2025-61882*, ORACLE, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html (last accessed Jan. 2, 2026).
[31] *Id.*
[32] *See id.*

39. As early as September 29, 2025, members of the CL0P ransomware group began contacting organizations and claiming to have stolen sensitive information from organizations' Oracle EBS environments.[33] Cybersecurity researchers discovered "additional suspicious activity dating back to July 10, 2025."[34]

40. CL0P is "a prolific ransomware family that has gained notoriety for its high-profile attacks."[35] CL0P is known for engaging in "double extortion" tactics where it steals and encrypts data before publishing the stolen data on its dark web leak site.[36] CL0P's "latest campaign targeting Oracle EBS marks a continuation of this successful and high-impact operational model."[37]

41. Reports indicate that CL0P has added UOPX to its dark web leak site.[38] Reports indicated CL0P's "focus was on exfiltrating data for extortion purposes."[39]

42. Defendants' failure to promptly notify Plaintiff and Class members that their PII was disclosed, accessed, and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII before Plaintiff and

---

[33] Peter Ukhanov et al., *Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign*, GOOGLE CLOUD (Oct. 9, 2025), https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation.

[34] *Id.*

[35] Trend Micro Research, *Ransomware Spotlight: Clop*, TREND MICRO (Aug. 31, 2023), https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop (last accessed Jan. 2, 2026).

[36] *See #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[37] Ukhanov et al., *supra* note 33.

[38] Steven Bowcut, *University of Phoenix Discloses 3.5M-Record Data Breach Linked to Oracle EBS Zero-Day*, BRILLIANCE SEC. MAG. (Dec. 29, 2025), https://brilliancesecuritymagazine.com/cybersecurity/university-of-phoenix-discloses-3-5m-record-data-breach-linked-to-oracle-ebs-zero-day/; *University of Phoenix Data Breach Exposes 3.5 Million in Oracle E-Business Suite (EBS) Zero-Day Attack*, RESCANA, https://www.rescana.com/post/university-of-phoenix-data-breach-exposes-3-5-million-in-oracle-e-business-suite-ebs-zero-day-atta (last accessed Jan. 2, 2026).

[39] *University of Phoenix Data Breach Exposes 3.5 Million*, *supra* note 38.

Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII

43. At all relevant times, Defendants knew, or should have known, that the PII that they collect, store, and share was a target for malicious actors. Despite such knowledge, Defendants failed, or shared PII with third parties that failed to, implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from unauthorized disclosures and cyberattacks that they should have anticipated and guarded against.

44. It is well known among companies that store sensitive personally identifying information that such information—such as the PII stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[40]

45. PII is a valuable property right.[41] The value of PII as a commodity is measurable.[42] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

[40] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[41] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[42] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[43] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[44] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

46. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

47. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[45]

48. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[43] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[44] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[45] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII Has Grave and Lasting Consequences for Victims

49. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[46] [47]

50. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[48]

51. Identity theft is not an easy problem to solve. In a 2025 survey, the Identity Theft Resource Center found that 20% of victims of identity misuse needed more than 30 days to resolve issues stemming from identity theft and 13% required three months or more.[49]

52. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

---

[46] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Jan. 2, 2026).

[47] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[48] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[49] Identity Theft Resource Center, *2025 Consumer Impact Report*, IDENTITY THEFT RES. CTR. (2025), https://www.idtheftcenter.org/publication/itrc-2025-consumer-impact-report/ (last accessed Jan. 2, 2026).

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[50]

53. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and Class Members

54. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the disclosure, compromise, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

55. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

56. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

---

[50] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

All persons whose PII was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

57. Plaintiff also brings this action on behalf of herself and all members of the following Subclasses of similarly situated persons:

UOPX Subclass
All persons who provided their PII to UOPX and whose PII was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

Illinois Subclass
All residents of Illinois whose PII was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

58. Excluded from the Class are The University of Phoenix, Inc., and its affiliates, parents, subsidiaries, employees, officers, agents, board members, and directors; Phoenix Education Partners, Inc., and its affiliates, parents, subsidiaries, employees, officers, agents, board members, and directors; Oracle Corporation, and its affiliates, parents, subsidiaries, employees, officers, agents, board members, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge.

59. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

60. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. UOPX reported to the Maine Attorney General that the Data Breach affected approximately 3,489,274 individuals.[51]

[51] University of Phoenix, Inc., *Data Breach Notification*, *supra* note 27.

61. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure;

b. whether Defendants had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;

c. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;

d. whether Defendants breached their duties to protect Plaintiff's and Class members' PII; and

e. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

62. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

63. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

64. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial

experience and success in the prosecution of complex consumer protection class actions of this nature.

65. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII in their possession, custody, or control.

68. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

69. Defendants' duties also arise from the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS. 530/45.

70. Additionally, under 815 ILCS 530/10, Defendants had a duty to "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach . . . in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10.

71. Defendants violated Section 5 of the FTCA and IPIPA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII, by failing to provide timely notice, and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtain and store, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

72. Defendants' violations of IPIPA and Section 5 of the FTCA constitute negligence per se.

73. UOPX also had duties to protect Plaintiff's and Class members' data under the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g. FERPA requires educational entities to obtain written consent prior to releasing any education records to anyone other than specific individuals or organizations listed in FERPA, none of which include cybercriminals. *See* 20 U.S.C. § 1232g(b)

74. UOPX's violations of FERPA constitute negligence per se.

75. Plaintiff and Class members are within the class of persons that IPIPA, Section 5 of the FTCA, and FERPA were intended to protect.

76. The harm occurring as a result of the Data Breach is the type of harm that IPIPA, Section 5 of the FTCA, and FERPA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Breach.

77. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted companies that collect and store PII in recent years.

78. Given the nature of Defendants' business, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendors inadequate data security and prevented the Data Breach from occurring or should not have provided PII to third-party vendors with inadequate data security.

79. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to, or failing to ensure that their third-party vendors, 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 PII entrusted to it—including Plaintiff's and Class members' PII.

80. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to, or failing to ensure that their third-party vendors, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

81. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

82. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT
Individually and on Behalf of the UOPX Subclass Against UOPX Only

83. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

84. Plaintiff brings this claim individually and on behalf of all other UOPX Subclass members against UOPX only.

85. In connection with receiving education, Plaintiff and all other UOPX Subclass members entered into implied contracts with UOPX.

86. Pursuant to these implied contracts, Plaintiff and UOPX Subclass members paid money to UOPX and provided UOPX with their PII. In exchange, UOPX agreed to, among other things, and Plaintiff and UOPX Subclass members understood that UOPX would: (1) provide education to Plaintiff and UOPX Subclass members; (2) collect, maintain, and utilize Plaintiff's and UOPX Subclass members' PII to, among other things, facilitate education to Plaintiff and UOPX Subclass members; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and UOPX Subclass members' PII; (4) protect Plaintiff's and UOPX Subclass members' PII in compliance with federal and state laws and regulations, industry standards, and UOPX's representations; and (5) maintain the confidentiality of Plaintiff's and UOPX Subclass members' PII and protect it from unauthorized access, disclosure, theft, and misuse.

87. The protection of PII was a material term of the implied contracts between Plaintiff and UOPX Subclass members, on the one hand, and UOPX, on the other hand. Indeed, as set forth *supra*, UOPX recognized the importance of data security and the privacy of its students' PII in its Privacy Policy. Had Plaintiff and UOPX Subclass members known that UOPX would not adequately protect its students' PII, they would not have agreed to provide UOPX with their PII or received education from UOPX.

88. Plaintiff and UOPX Subclass members performed their obligations under the implied contract when they provided UOPX with their PII and paid for education from UOPX.

89. UOPX breached its obligations under its implied contracts with Plaintiff and UOPX Subclass members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain reasonable security protocols and procedures to protect Plaintiff's and UOPX Subclass members' PII in a manner that complies with applicable laws, regulations, industry standards, and UOPX's representations.

90. UOPX's breach of its obligations of its implied contracts with Plaintiff and UOPX Subclass members directly resulted in the Data Breach and the injuries that Plaintiff and all other UOPX Subclass members have suffered from the Data Breach.

91. Plaintiff and all other UOPX Subclass members were damaged by UOPX's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT III
UNJUST ENRICHMENT

92. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

93. This claim is pleaded in the alternative to the breach of implied contract claim.

94. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for education (directly or indirectly) and through the provision of their PII.

95. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII, as this was used to facilitate educational services.

96. As a result of Defendants' conduct, UOPX's current and former students suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that students paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

97. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

98. Plaintiff and Class members have no adequate remedy at law.

99. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT IV
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/2, et seq. ("ICFA")
Individually and on Behalf of the Illinois Subclass

100. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

101. Plaintiff brings this claim individually and on behalf of all other Illinois Subclass members against Defendants.

102. Defendants offered and continues to offer education services in the State of Illinois.

103. Plaintiff and Illinois Subclass members purchased and received education from UOPX for personal, family, or household purposes.

104. Defendants engaged in unlawful and unfair practices in violation of ICFA by failing to implement and maintain reasonable security measures to protect and secure their students' or their clients' students' PII in a manner that complied with applicable laws, regulations, industry standards, and Defendants' representations.

105. Defendants make explicit statements to their students and clients that their PII will remain private.

106. Defendants' duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. Defendants violated this duty by failing to implement reasonably secure data security policies.

107. Defendants further violated ICFA by failing to notify their current and former students or clients' students of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under ICFA. 815 ILCS 530/20.

108. Due to the Data Breach, Plaintiff and Illinois Subclass members have lost property in the form of their PII. Further, Defendants' failure to, or failure to ensure their third-party vendors, adopt reasonable practices in protecting and safeguarding their students' or clients' students' PII will force Plaintiff and Illinois Subclass members to spend time or money to protect against identity theft. Plaintiff and Illinois Subclass members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information or contracting with entities that collect and store PII without appropriate and reasonable safeguards to protect such information.

109. As a result of Defendants' violations of ICFA, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 5, 2026

Respectfully submitted,

/s/ Bruce W. Steckler

Bruce W. Steckler
STECKLER WAYNE & LOVE PLLC
12720 Hillcrest Suite 1045
Dallas, Texas 75230
Tel: 972.387.4040
bruce@stecklerlaw.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Counsel for Plaintiff

**Pro hac vice* forthcoming

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Tiaa Pointer, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Cook County, IL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Steckler Wayne & Love PLLC; 12720 Hillcrest Road, Suite 1045, Dallas, TX 75230; 972-387-4040

DEFENDANTS

The University of Phoenix, Inc., Phoenix Education Partners, Inc., and Oracle Corporation

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d) - Class Action Fairness Act

Brief description of cause:
Putative class action relating to flight cancellation and delays due to an airline computer system outage caused by Defendant.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ >$5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon. Alan D. Albright DOCKET NUMBER 1:25-cv-01999

DATE 01/05/2026

SIGNATURE OF ATTORNEY OF RECORD /s/ Bruce W. Steckler

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.