UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE ORACLE CORPORATION DATA BREACH LITIGATION This Document Relates To: ALL ACTIONS	Master File No. 1:25-cv-01805-ADA-SH

CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

I. NATURE OF ACTION 1
II. PARTIES 2
Plaintiffs 2
Defendants 6
III. JURISDICTION AND VENUE 7
IV. BACKGROUND 8
Defendant Oracle Corporation and Oracle E-Business Suite 8
The Russian Cybercriminal Syndicate CL0P 15
The Data Breach, Cl0p, and the CVE-2025-61882 Vulnerability 19
Defendant Anywhere Real Estate Inc. 26
Defendant Cox Enterprises, Inc. 30
GlobalLogic Inc. 34
Defendant LKQ Corporation 38
Defendant Madison Square Garden Entertainment Corp. 41
Defendant Parexel International, LLC 45
Defendant The Research Foundation for The State University of New York 48
Defendant Trustees of Dartmouth College 52
Defendant University of Pennsylvania 56
Defendant University of Phoenix 59
Defendant WP Company LLC 63
V. EXPERIENCES AND INJURIES OF PLAINTIFFS 67
Plaintiff Matthew Tannehill 67
Plaintiff Michael Nero 70
Plaintiff James Massengill 72
Plaintiff Marcus Issac 75
Plaintiff Leonid Koyfman 78
Plaintiff Micheil Boggs 80
Plaintiff Patricia Eagan 83
Plaintiff Ashley Sainvil 86
Plaintiff Lisa Magnusson 88
Plaintiff Arianna Brown 91

Plaintiff KaSandra Reynolds 94
Plaintiff Christian Alvarado 97
Plaintiff Angel Liranzo 99
Plaintiff Kevin Youmell 102
Plaintiff Michael Trempus 104
Plaintiff Nicole O'Keeffe 107
Plaintiff Lourdes Naulty 110
Plaintiff Richard Yao 113
Plaintiff Matthew Ross 116
Plaintiff Lisa Mabey 118
Plaintiff Maxim Gilula 121
Plaintiff Thomas Mosby 125
Plaintiff Stacy Ranson 127
Plaintiff Tiaa Pointer 130
Plaintiff Luis Vega 133
Plaintiff Antonyo Wyche 136
Plaintiff Sarah Clark 139
Plaintiff Anthony Bryant 142
Plaintiff Bruce Bennett 145
Plaintiff James Nance 148
Plaintiff Rachel Hatzipanagos 151
Plaintiff Richard Leiby 153
Plaintiff Jun Hee Kim 156
VI. COMMON ALLEGATIONS 159
Consumers Prioritize Data Security 159
Substantially Increased Risk of Identity Theft and Fraud 161
Defendants Knew—Or Should Have Known—of the Risk of a Data Breach 167
Defendants Could Have Prevented the Data Breach 168
Defendants Failed to Follow FTC Guidelines 169
Defendants Failed to Follow Industry Standards 170
VII. CLASS ACTION ALLEGATIONS 171
VIII. CAUSES OF ACTION 178

Count I – Negligence 178
Count II – Invasion of Privacy 183
Count III – Violations of the California Consumer Privacy Act 185
Count IV– Violation of the California Customer Records Act 187
IX. PRAYER FOR RELIEF 188
X. DEMAND FOR JURY TRIAL 189

Plaintiffs Matthew Tannehill, Michael Nero, James Massengill, Marcus Issac, Leonid Koyfman, Micheil Boggs, Patricia Eagan, Ashley Sainvil, Lisa Magnusson, Arianna Brown, KaSandra Reynolds, Christian Alvarado, Kevin Youmell, Michael Trempus, Nicole O'Keeffe, Lourdes Naulty, Richard Yao, Matthew Ross, Lisa Mabey, Maxim Gilula, Thomas Mosby, Stacy Ranson, Tiaa Pointer, Luis Vega, Antonyo Wyche, Anthony Bryant, Bruce Bennett, James Nance, Rachel Hatzipanagos, Richard Leiby, Jun Hee Kim, Angel Liranzo, and Sarah Clark ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendants Anywhere Real Estate Inc., Cox Enterprises, Inc., LKQ Corporation, Madison Square Garden Entertainment Corp., Oracle Corporation, Parexel International, LLC, The Research Foundation for The State University of New York, Trustees of Dartmouth College d/b/a Dartmouth College, The Trustees of the University of Pennsylvania d/b/a University of Pennsylvania, University of Phoenix, Inc., and WP Company LLC d/b/a The Washington Post ("Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, investigations of counsel, and facts of public record.

I. NATURE OF ACTION

1. Plaintiffs and Class Members bring this Complaint as a result of Defendants' failure to adequately protect the confidential personal and financial information that they obtained from Plaintiffs and Class Members—including, for example, Social Security numbers and financial account information like bank account numbers and routing numbers.

2. As a result of Defendants' failure to adhere to industry standards and implement reasonable data security measures, the Russian cybercriminal syndicate "CL0P" acquired the

private information of Plaintiffs and Class Members during a targeted data breach in or around August 2025 (the "Data Breach").

3. CL0P then leaked the private information of Plaintiffs and Class Members on its Dark Web leak site called "CL0P^_-LEAKS."

4. In the aftermath of their exposure, Plaintiffs suffered numerous injuries—including, *inter alia*, identity theft, fraudulent charges on their financial accounts, privacy injuries, emotional injuries, lost time, and out-of-pocket costs, including the costs for identity and credit monitoring services purchased as a result of the Data Breach.

5. To remedy these injuries, Plaintiffs bring this class action on behalf of themselves, and all others similarly situated (the "Class" or "Class Members").

II. PARTIES

Plaintiffs

6. Plaintiff, Matthew Tannehill, is a natural person and a citizen of Texas. He is domiciled in Texas (where he intends to remain). He is a former employee of Anywhere.

7. Plaintiff, Michael Nero, is a natural person and a citizen of Connecticut. He is domiciled in Connecticut (where he intends to remain). He is a former employee of Anywhere.

8. Plaintiff James Massengill is a natural person and a citizen of Virginia. He is domiciled in Virginia (where he intends to remain). He is a former employee of Cox.

9. Plaintiff Marcus Issac is a natural person and a citizen of Texas. He is domiciled in Texas (where he intends to remain). He is a former employee of Cox.

10. Plaintiff Leonid Koyfman is a natural person and a citizen of California. He is domiciled in California (where he intends to remain). He is a former employee of GlobalLogic.

11. Plaintiff Micheil Boggs is a natural person and a citizen of Oklahoma. He is domiciled in Oklahoma (where he intends to remain). Through the intermediary Braven Inc., he is a former employee or contractor of GlobalLogic.

12. Plaintiff Patricia Eagan is a natural person and a citizen of California. She is domiciled in California (where she intends to remain). She is a former employee or contractor of GlobalLogic.

13. Plaintiff Ashley Sainvil is a natural person and a citizen of New York. She is domiciled in New York (where she intends to remain). She is a current employee of GlobalLogic.

14. Plaintiff Lisa Magnusson is a natural person and a citizen of Texas. She is domiciled in Texas (where she intends to remain). She is a former employee of GlobalLogic.

15. Plaintiff Arianna Brown is a natural person and a citizen of New York. She is domiciled in New York (where she intends to remain). She is a former employee of GlobalLogic.

16. Plaintiff KaSandra Reynolds is a natural person and a citizen of Washington. She is domiciled in Washington (where she intends to remain). She is a former employee of LKQ.

17. Plaintiff Christian Alvarado is a natural person and a citizen of California. He is domiciled in California (where he intends to remain). He is a former employee of MSG.

18. Plaintiff Kevin Youmell is a natural person and a citizen of Massachusetts. He is domiciled in Massachusetts (where he intends to remain). He is a former employee of Parexel.

19. Plaintiff Michael Trempus is a natural person and a citizen of North Carolina. He is domiciled in North Carolina (where he intends to remain). He is a former employee of Parexel.

20. Plaintiff Nicole O'Keeffe is a natural person and a citizen of Texas. She is domiciled in Texas (where she intends to remain). She is a former employee of Parexel.

21. Plaintiff Lourdes Naulty is a natural person and a citizen of Maryland. She is domiciled in Maryland (where she intends to remain). She is a former employee of Parexel.

22. Plaintiff Richard Yao is a natural person and a citizen of New York. He is domiciled in New York (where he intends to remain). He is a former graduate student of RF SUNY.

23. Plaintiff Matthew Ross is a natural person and a citizen of Massachusetts. He is domiciled in Massachusetts (where he intends to remain). He is a former student of Dartmouth.

24. Plaintiff Lisa Mabey is a natural person and a citizen of New Hampshire. She is domiciled in New Hampshire (where she intends to remain). She is a former patient of the Dartmouth Hitchcock Medical Center.

25. Plaintiff Maxim Gilula is a natural person and a citizen of California. He is domiciled in California (where he intends to remain). He is a former student of the University of Pennsylvania.

26. Plaintiff Thomas Mosby is a natural person and a citizen of Arizona. He is domiciled in Arizona (where he intends to remain). He is a current employee of the University of Phoenix.

27. Plaintiff Stacy Ranson is a natural person and a citizen of Illinois. She is domiciled in Illinois (where she intends to remain). She is a former student and employee of the University of Phoenix.

28. Plaintiff Tiaa Pointer is a natural person and a citizen of Illinois. She is domiciled in Illinois (where she intends to remain). She is a former student of the University of Phoenix.

29. Plaintiff Luis Vega is a natural person and a citizen of Texas. He is domiciled in Texas (where he intends to remain). He is a former employee of the University of Phoenix.

30. Plaintiff Antonyo Wyche is a natural person and a citizen of Georgia. He is domiciled in Georgia (where he intends to remain). He is a former student of the University of Phoenix.

31. Plaintiff Anthony Bryant is a natural person and a citizen of Virginia. He is domiciled in Virginia (where he intends to remain). He is a current employee of the Washington Post.

32. Plaintiff Bruce Bennett is a natural person and a citizen of Arizona. He is domiciled in Arizona (where he intends to remain). He is a former employee of the Washington Post.

33. Plaintiff James Nance is a natural person and a citizen of Colorado. He is domiciled in Colorado (where he intends to remain). He is a former employee of the Washington Post.

34. Plaintiff Rachel Hatzipanagos is a natural person and a citizen of Maryland. She is domiciled in Maryland (where she intends to remain). She is a current employee of the Washington Post.

35. Plaintiff Richard Leiby is a natural person and a citizen of the District of Columbia. He is domiciled in the District of Columbia (where he intends to remain). He is a former employee of the Washington Post.

36. Plaintiff Jun Hee Kim is a natural person and a citizen of Maryland. He is domiciled in Maryland (where he intends to remain). He is a former employee of the Washington Post.

37. Plaintiff Angel Liranzo is a natural person and a citizen of New Jersey. She is domiciled in New Jersey (where she intends to remain). She is a former employee of Madison Square Garden.

38. Plaintiff Sarah Clark is a natural person and a citizen of Michigan. She is domiciled in Michigan (where she intends to remain). She is a former employee of the University of Phoenix.

Defendants

39. Defendant Anywhere Real Estate Inc. ("Anywhere") is a corporation incorporated in Delaware and with its principal place of business at 175 Park Ave, Madison, New Jersey 07940.

40. Defendant Cox Enterprises, Inc. ("Cox") is a corporation incorporated in Delaware and with its principal place of business at 6205 Peachtree Dunwoody Road, Atlanta, Georgia 30328.

41. Defendant LKQ Corporation ("LKQ") is a corporation incorporated in Delaware and with its principal place of business at 5846 Crossings Blvd, Antioch, Tennessee 37013.

42. Defendant Madison Square Garden Entertainment Corp. ("MSG") is a corporation incorporated in Nevada and with its principal place of business at 2 Pennsylvania Plaza, New York, New York 10121.

43. Defendant Oracle Corporation ("Oracle") is a corporation incorporated in Delaware and with its principal place of business at 2300 Oracle Way, Austin, Texas 78741.

44. Defendant Parexel International, LLC ("Parexel") is a limited liability company formed under the laws of Delaware and with its principal place of business at 275 Grove Street, Suite 1E-310, Newton, Massachusetts 02466. The sole member of Parexel International, LLC is PAREXEL International (MA) Corporation which is a corporation incorporated in Massachusetts and with its principal place of business at 275 Grove Street, Suite 1E-310, Newton, Massachusetts 02466.

45. Defendant The Research Foundation for The State University of New York ("RF SUNY") is a non-profit educational corporation incorporated in New York and with its principal place of business at 35 State Street Albany, New York 12207.

46. Defendant Trustees of Dartmouth College d/b/a Dartmouth College ("Dartmouth") is a non-profit incorporated in New Hampshire and with its principal place of business at 7 Lebanon Street, Hanover, New Hampshire 03755.

47. Defendant The Trustees of the University of Pennsylvania d/b/a University of Pennsylvania ("UPenn") is a non-profit corporation incorporated in Pennsylvania and with its principal place of business at 3451 Walnut Street, 5th Floor Franklin Bldg., Philadelphia, Pennsylvania 19104.

48. Defendant University of Phoenix, Inc. ("University of Phoenix") is a corporation incorporated in Arizona and with its principal place of business at 4035 S. Riverpoint Parkway, Phoenix, Arizona.

49. Defendant WP Company LLC d/b/a The Washington Post ("Washington Post") is a limited liability company formed under the laws of Delaware and with its principal place of business at 1301 K Street NW, Washington, DC, 20005.

III. JURISDICTION AND VENUE

50. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Many Plaintiffs and Defendants are citizens of different states. And there are over one-hundred putative Class Members.

51. This Court has personal jurisdiction over Defendants because they have sufficient minimum contacts in Texas. The corporate headquarters of Defendant Oracle Corporation is in Texas, and the other Defendants conducted substantial business in Texas with Defendant Oracle Corporation. On information and belief, all Defendants (besides Oracle Corporation) purposefully

transmitted the Private Information of Plaintiffs and Class Members to Oracle Corporation in Texas.

52. Venue is proper in this Court because the corporate headquarters of Defendant Oracle Corporation is in this District and because a substantial part of the events, acts, and omissions giving rise to the claims of Plaintiffs occurred in this District. On information and belief, all Defendants (besides Oracle Corporation) purposefully transmitted the Private Information of Plaintiffs and Class Members to Oracle Corporation in this District.

IV. BACKGROUND

Defendant Oracle Corporation and Oracle E-Business Suite

53. Defendant Oracle is "a cloud technology company that provides organizations around the world with computing infrastructure and software[.]"[1]

54. Relevant here, is the Oracle E-Business Suite ("Oracle EBS") which Oracle advertises as "a complete set of business applications for managing and automating processes across your enterprise."[2]

55. Oracle explains that "[t]housands of organizations around the world rely on Oracle E-Business Suite to run their key business operations."[3]

[1] *Oracle: About*, LINKEDIN, https://www.linkedin.com/company/oracle/about/ (last visited Feb. 26, 2026).
[2] *Oracle® E-Business Suite User's Guide*, ORACLE, https://docs.oracle.com/cd/E18727_01/doc.121/e12896/T27641T27643.htm (last visited Feb. 26, 2026).
[3] *Oracle E-Business Suite*, ORACLE, https://www.oracle.com/applications/ebusiness/ (last visited Feb. 26, 2026).

56. Oracle EBS includes a suite of different products focused on: "Order Management, Logistics, Procurement, Projects, Manufacturing, Asset Lifecycle Management, Service, Financials, Human Capital Management."[4]

57. For example, Oracle advertises that the "Human Capital Management" portion of Oracle EBS includes the following products:

a. "Advanced Benefits (PDF) Manage and deliver benefits programs which meet your mission and objectives using sophisticated and configurable Life Event management and scheduled processing capabilities along with flexible and extendable rate and premium calculations. Offer employees the ability to update and review their own benefit data via self-service enrollment. Direct integration with Oracle EBS Core HR and Payroll applications streamlines processing."[5]

b. "Compensation Workbench (PDF) Give managers and compensation professionals the tools to strategically manage compensation at a global level. Use compensation to enhance productivity, increase morale and retain highly valued employees within an environment that enforces fiscal discipline and corporate policies."[6]

c. "Configuration Workbench (PDF) An integrated configuration management toolset for HR systems that makes it possible to lower the total cost of ownership during implementation and throughout the application lifecycle. The Workbench provides a unified and consistent framework to

[4] *Id*. (adding punctuation marks).
[5] *Id*.
[6] *Id*.

assist in the evaluation, configuration, deployment and maintenance of sophisticated HRMS applications."[7]

d. "Human Resources (PDF) Use this powerful tool to optimize the human assets of your business, whether you operate in the private or public sector. It allows you to adopt structured approaches to attracting, retaining, and developing talent along with encouraging the critical skills and knowledge needed to improve the capability of your business to meet new challenges."[8]

e. "iRecruitment (PDF) A full-cycle recruiting solution focused on the manager-recruiter-candidate hiring relationship that fully automates the entire recruitment process. Oracle iRecruitment works seamlessly with the Oracle Human Resource Management System (HRMS) to manage the entire workforce lifecycle."[9]

f. "Payroll (PDF) A high-performance, graphical, rules-based payroll management system that is designed to keep pace with the changing needs of your enterprise and workforce in order to reduce setup costs, administrative and processing errors."[10]

g. "Self Service Human Resources (PDF) Enable your workforce to manage information through interfaces personalized to their roles, on-line experience, work content, language, and information needs. The flexible

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

> and intuitive user interface is designed for the novice user, with easy-to-use navigation, graphics along with helpful tips."[11]

58. In the regular course of its business, Oracle obtains the personally identifiable information ("PII" or "Private Information") of millions of people—including, but not limited to, names, dates of birth, Social Security numbers, driver's license numbers, passport numbers, government ID numbers, tax ID numbers, contact information, telephone numbers, email addresses, physical addresses, financial account information (including routing numbers and account numbers), and payment card numbers (e.g., debit card numbers, credit card numbers).

59. The other Defendants are enterprise clients of Oracle, and they used Oracle EBS to manage and store the Private Information of their current and former employees, contractors, students, consumers, and/or customers (i.e., "Class Members" or the "Class").

60. The Oracle client Defendants provided Oracle with sensitive and confidential personal information through the Oracle EBS platform and Oracle thus also obtained the Private Information of these current and former employees, contractors, students, consumers, and/or customers.

61. In collecting and maintaining the Private Information, Defendants agreed they would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information.

62. Under state and federal law, businesses like Defendants have duties to protect the Private Information of their employees, contractors, students, and customers, and to notify them about data breaches.

---

[11] *Id.*

63. Oracle recognizes these duties, and advertises in its "General Privacy Policy" that:

a. "Oracle Corporation and its affiliated entities are responsible for processing your personal information described in this Privacy Policy."[12]

b. "Oracle has implemented appropriate technical, physical and organizational measures designed to protect personal information against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, as well as all other forms of unlawful processing."[13]

c. "As used in this Privacy Policy, 'personal information' or 'personal data' means information that relates to an identified individual or to an identifiable individual."[14]

d. "Specific pieces of information about you that Oracle may collect and process depending on your interaction with Oracle, includes: name and physical address, email addresses, and telephone numbers; demographic attributes, when tied to personal information that identifies you; photographs that identify you and testimonials; public information about your work and education history, including professional affiliations; information you provide on your public social media profiles related to your professional and educational history, such as LinkedIn; transactional data, including products and services ordered, financial details and payment methods; company data such as the name, size and location of the company

[12] *Oracle General Privacy Policy*, ORACLE (Oct. 10, 2024) https://www.oracle.com/legal/privacy/privacy-policy/.
[13] *Id*.
[14] *Id*

you work for and your role within the company as well as publicly available company information and activity associated with company data; data from surveys conducted by Oracle or by third parties on behalf of Oracle and publicly available information, such as social media posts; call recording and chat transcript data from Sales and customer support calls and live chat sessions or interviews; unique IDs such as your mobile device identifier or cookie ID on your browser; IP address and information that may be derived from IP address, such as geographic location; information about a device you use, such as browser, device type, operating system, the presence or use of 'apps', screen resolution, and the preferred language; certain location or geolocation information you provide directly or through automated means, if you choose to enable location based services from your device or Oracle app; and behavioral data of the internet connected computer or device you use when interacting with the sites, such as advertisements clicked or viewed, sites and content areas, date and time of activities or the web search used to locate and navigate to a site."[15]

64. Furthermore, Oracle advertises in its current "Oracle Services Privacy Policy" that:

a. "Oracle has implemented and will maintain technical and organizational measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Services Personal Information." [16]

[15] *Id*. (cleaned up).
[16] *Oracle Services Privacy Policy*, ORACLE (Feb. 25, 2026) https://www.oracle.com/legal/privacy/services-privacy-policy/.

b. "These measures, which are generally aligned with the ISO/IEC 27001:2013 standard, govern all areas of security applicable to the Services, including physical access, system access, data access, transmission, input, security oversight, and enforcement."[17]

c. "Oracle employees are required to maintain the confidentiality of personal information. Employees' obligations include written confidentiality agreements, regular training on information protection, and compliance with company policies concerning protection of confidential information."[18]

d. "Oracle promptly evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or handling of Services Personal Information."[19]

e. "If Oracle becomes aware and determines that an incident involving Services Personal Information qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Services Personal Information transmitted, stored or otherwise processed on Oracle systems that compromises the security, confidentiality or integrity of such Services Personal Information, Oracle will report such breach to You ***without undue delay***."[20]

[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*. (emphasis added).

f. "Oracle has implemented appropriate technical, physical and organizational measures in accordance with the Oracle Corporate Security Practices designed to protect personal information against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing."[21]

The Russian Cybercriminal Syndicate CL0P

65. As explained herein, the Data Breach was initiated by the notorious Russian cybercriminal syndicate "CL0P" (also known as "Cl0p" and "CLOP" and "Clop"). [22]

66. The involvement of CL0P is significant, and the global cybersecurity firm Barracuda has reported that:

a. "Cl0p ransomware is a private ransomware operation run by an organized cybercrime group known as TA505. The Cl0p operation is just one of several units of the TA505 criminal enterprise, and it is thought to be the most profitable."[23]

b. "Since its emergence in 2019, Cl0p has extorted over $500 million in ransom payments and has directly affected thousands of organizations and tens of millions of individuals globally."[24]

[21] *Id*.
[22] *See infra*.
[23] Christine Barry, *Cl0p ransomware: The skeezy invader that bites while you sleep*, BARRACUDA (May 16, 2025) https://blog.barracuda.com/2025/05/16/cl0p-ransomware--the-skeezy-invader-that-bites-while-you-sleep.
[24] *Id*.

c. "In the final quarter of 2024, Cl0p outpaced Akira and overtook RansomHub to become the most active ransomware group in the landscape."[25]

d. "In the first quarter of 2025, Cl0p surpassed LockBit as the most prolific ransomware group, based on publicly disclosed breaches."[26]

e. "Researchers believe the brand name comes from the Russian word 'клоп', or 'klop,' which translates to 'bedbug' in English."[27]

f. "Researchers put TA505 and Cl0p ransomware in Russia or the Commonwealth of Independent States (CIS)."[28]

g. "Cl0p ransomware is specifically programmed not to execute on Russian-language systems, and the group's communications and code comments contain Russian language elements and cultural references."[29]

h. "Command-and-control servers and payment infrastructure elements have been traced back to Russia and Eastern Europe."[30]

67. The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a joint "Cybersecurity Advisory (CSA)" on CL0P—warning the public that:

a. "Appearing in February 2019, and evolving from the CryptoMix ransomware variant, CL0P was leveraged as a Ransomware as a Service

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*

(RaaS) in large-scale spear-phishing campaigns that used a verified and digitally signed binary to bypass system defenses."[31]

b. "CL0P was previously known for its use of the 'double extortion' tactic of stealing and encrypting victim data, refusing to restore victim access and publishing exfiltrated data on Tor via the CL0P^_-LEAKS website."[32]

c. "Beyond CL0P ransomware, TA505 is known for frequently changing malware and driving global trends in criminal malware distribution."[33]

d. "Considered to be one of the largest phishing and malspam distributors worldwide, TA505 is estimated to have compromised more than 3,000 U.S.-based organizations and 8,000 global organizations."[34]

68. CL0P is notorious for disseminating stolen data on the Dark Web. And since at least 2020, CL0P has operated a data leak site called "CL0P^_- LEAKS" on the Dark Web.[35]

69. For context, the "Dark Web" is the "part of the internet where users can access unindexed web content anonymously through special web browsers like The Onion Router (Tor)."[36] The Dark Web is anonymous, unregulated, and an "appealing tool for cybercriminals[.]"[37]

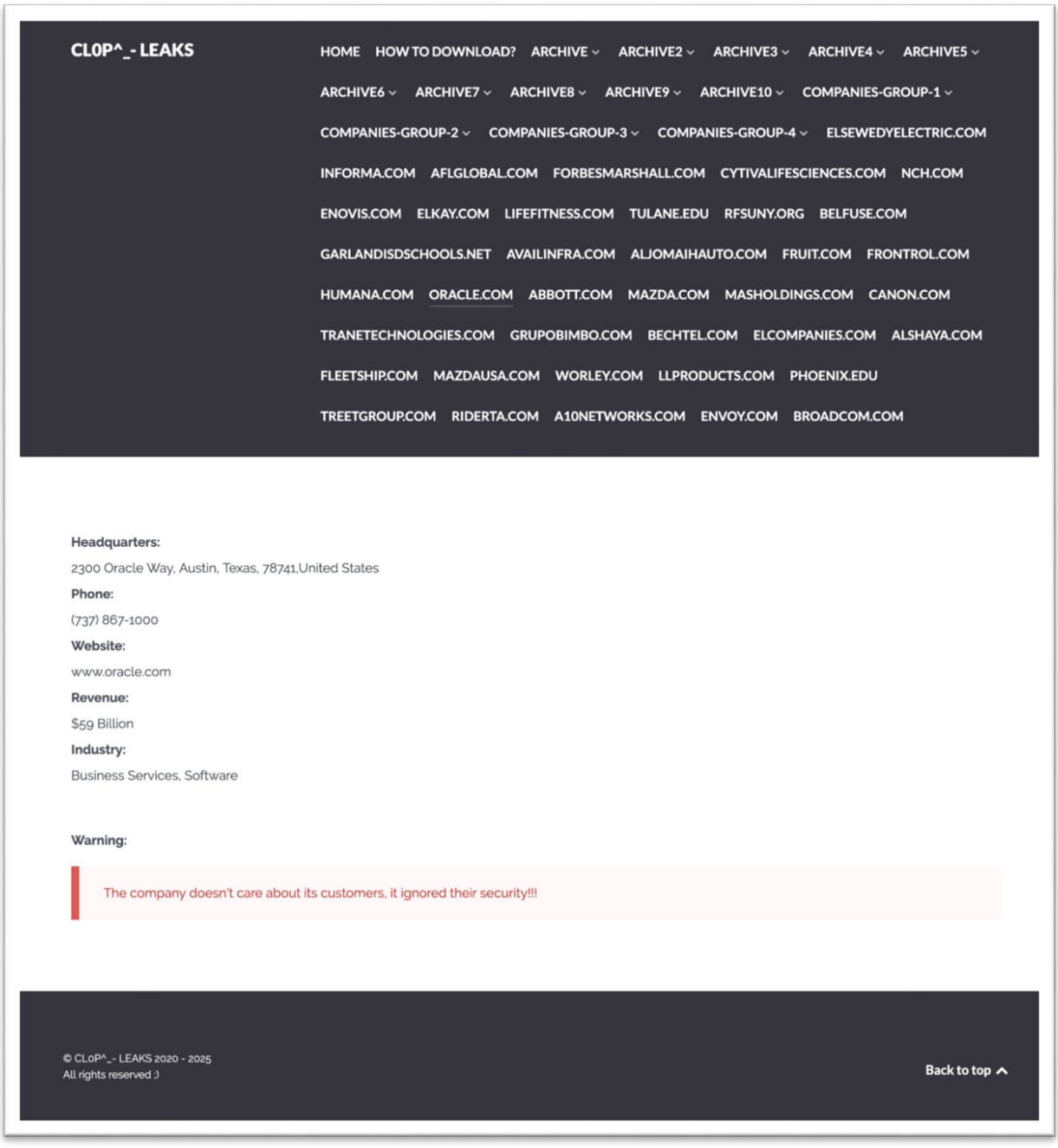
---

[31] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 13, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.
[32] *Id*.
[33] *Id*.
[34] *Id*.
[35] *Id*.
[36] Kurt Baker, *The Dark Web Explained*, CROWDSTRIKE (Feb. 11, 2025) https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/.
[37] *Id*.

70. In recent years, "the majority of the alleged victims [on CL0P^_- LEAKS] appear to be associated with data theft extortion incidents stemming from the mass exploitation of zero-day vulnerabilities in managed file transfer (MFT) systems, including the Accellion legacy file transfer appliance (FTA), GoAnywhere MFT, MOVEit MFT, and Cleo LexiCom."[38] And "[i]n most of these incidents, the threat actors conducted mass exploitation of zero-day (0-day) vulnerabilities, stole victim data, then initiated extortion attempts several weeks later."[39]

[38] 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.
[39] *Id*.

71. An example screenshot of the CL0P^_- LEAKS website is provided below.[40]



The Data Breach, Cl0p, and the CVE-2025-61882 Vulnerability

[40] *ORACLE*, RANSOM LOOK (Nov. 20, 2025) https://www.ransomlook.io/screenshots/clop/ORACLECOM.png.

72. On or before August 9, 2025, the cybercriminal syndicate CL0P exploited a vulnerability in the Oracle EBS software and then targeted and exfiltrated the Private Information of Plaintiffs and Class Members (i.e., the Data Breach).[41]

73. The vulnerability in Oracle EBS that CL0P exploited during the Data Breach is called "CVE-2025-61882."[42]

74. On October 4, 2025, Oracle issued a "Security Alert Advisory" providing information about the Data Breach and the CVE-2025-61882 vulnerability:

a. "This Security Alert addresses vulnerability CVE-2025-61882 in Oracle E-Business Suite."[43]

b. "This vulnerability is ***remotely exploitable without authentication***, i.e., it may be exploited over a network without the need for a username and password."[44]

c. "If successfully exploited, this vulnerability may result in remote code execution."[45]

d. "Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible."[46]

e. "Affected Products and Versions: Oracle E-Business Suite, versions 12.2.3-12.2.14."

---

[41] *See* 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.
[42] *Id*.
[43] *Oracle Security Alert Advisory - CVE-2025-61882*, ORACLE, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html (last visited Feb. 26, 2026).
[44] *Id*. (emphasis added).
[45] *Id*.
[46] *Id*.

f. "Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Security Alert. However, it is likely that earlier versions of affected releases are also affected by these vulnerabilities."[47]

75. Therein, Oracle published a "Risk Matrix" which provided key metrics about the Data Breach.[48] A screenshot of the Risk Matrix is provided below.[49]

CVE ID	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected
		Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability	
CVE-2025-61882	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	12.2.3-12.2.14

76. Notably, the Risk Matrix marked the Data Breach with a "Base Score" of 9.8.[50] This is significant because the Base Score is "an assessment of risk" and "a numeric value between 0.0 and 10.0 which indicates the relative severity of the vulnerability, where 10.0 represents the highest severity."[51]

77. Furthermore, in the Security Alert Advisory, Oracle implicitly confirmed the involvement of CL0P because Oracle admitted that the "Indicators of Compromises" included the following texts:

a. "oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_***cl0p***_

[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Risk Matrix Glossary – Terms and Definitions for Critical Patch Update Risk Matrices*, ORACLE (Oct. 2020) https://www.oracle.com/security-alerts/advisorymatrixglossary.html.

hunters.zip"[52]

b. "oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-***cl0p***_hunters/exp.py"[53]

c. "oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-***cl0p***_hunters/server.py"[54]

78. On October 9, 2025, the cybersecurity firm Mandiant Consulting ("Mandiant") and Google Threat Intelligence Group ("Google") published a "Threat Intelligence" report about the Data Breach.[55]

79. Notably, Mandiant worked with Oracle to address the Data Breach—and Oracle issued a "Credit Statement" that credited Mandiant "for contributions related to the security vulnerability[.]"[56]

80. In the Threat Intelligence report, Mandiant and Google reported the following:

a. "Beginning Sept. 29, 2025, Google Threat Intelligence Group (GTIG) and Mandiant began tracking a new, large-scale extortion campaign by a threat actor claiming affiliation with the CL0P extortion brand."[57]

---

[52] *Oracle Security Alert Advisory - CVE-2025-61882*, ORACLE, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html (last visited Feb. 26, 2026).
[53] *Id*. (emphasis added).
[54] *Id*. (emphasis added).
[55] *Id*. (emphasis added).
[56] *Oracle Security Alert Advisory - CVE-2025-61882*, ORACLE, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html (last visited Feb. 26, 2026) ("Credit Statement Oracle acknowledges the following organizations for contributions related to the security vulnerability addressed by this Security Alert: CrowdStrike Mandiant.").
[57] 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.

b. "The actor began sending a high volume of emails to executives at numerous organizations, alleging the theft of sensitive data from the victims' Oracle E-Business Suite (EBS) environments."[58]

c. "On Oct. 2, 2025, Oracle reported that the threat actors may have exploited vulnerabilities that were patched in July 2025 and recommended that customers apply the latest critical patch updates."[59]

d. "Our analysis indicates that the CL0P extortion campaign followed ***months of intrusion activity*** targeting EBS customer environments."[60]

e. "The threat actor(s) exploited what may be CVE-2025-61882 as a zero-day vulnerability against Oracle EBS customers as early as Aug. 9, 2025, weeks before a patch was available, with additional suspicious activity dating back to July 10, 2025."[61]

f. "In some cases, the threat actor ***successfully exfiltrated a significant amount of data*** from impacted organizations."[62]

81. Mandiant and Google also reported that CL0P launched an extortion campaign:

a. "Starting Sept. 29, 2025, the threat actor launched a high-volume email campaign from hundreds, if not thousands, of compromised third-party accounts. The credentials for these accounts—which belong to diverse, unrelated organizations—were likely sourced from infostealer malware logs sold on underground forums. This is a common tactic used by threat

[58] *Id*.
[59] *Id*.
[60] *Id*. (emphasis added).
[61] *Id*.
[62] *Id*. (emphasis added).

actors to add legitimacy and bypass spam filters. The emails, sent to company executives, claimed the actor had breached their Oracle EBS application and exfiltrated documents."[63]

b. "To substantiate their claims, the threat actor has provided legitimate file listings from victim EBS environments to multiple organizations with data dating back to mid-August 2025. The extortion emails have indicated that alleged victims can prevent the release of stolen data in exchange for payment, but the amount and method has not been specified. This is typical of most modern extortion operations, in which the demand is typically provided after the victim contacts the threat actors and indicates that they are authorized to negotiate."[64]

82. In the extortion demands, CL0P stated, *inter alia*, that:

a. "We have recently breached your Oracle E-Business Suite application and copied a lot of documents."[65]

b. "All the private files and other information are now held on our systems."[66]

c. "So, your only option to protect your business reputation is to discuss conditions and pay claimed sum. In case you refuse, you will lose all abovementioned data: some of it will be sold to the black actors, the rest will be published on our blog and shared on torrent trackers."[67]

[63] *Id*.
[64] *Id*.
[65] *Id*.
[66] *Id*.
[67] *Id*.

d. "As evidence, we can show any 3 files you ask or data row."[68]

e. "Time is ticking on clock and in few days if no payment we publish and close chat."[69]

83. The exact starting date of the Data Breach is unclear—and Mandiant and Google detected "additional suspicious activity dating back to July 10, 2025."[70] Thus, on information and belief, the Data Breach began before August 9, 2025, and possibly even before July 10, 2025.

84. Thus far, the precise scope of the Data Breach is unclear. But on information and belief, the types of Private Information that CL0P obtained from Oracle EBS during that Data Breach, include, at minimum: names, dates of birth, Social Security numbers, driver's license numbers, passport numbers, government ID numbers, tax ID numbers, contact information, telephone numbers, email addresses, physical addresses, financial account information (including routing numbers and account numbers), and payment card numbers (e.g., debit card numbers, credit card numbers).

85. Over the following months, CL0P began leaking vast amounts of Oracle EBS data on its Dark Web leak site CL0P^_- LEAKS.[71] In doing so, CL0P leaked the data of "more than 100 organizations" on the Dark Web.[72]

86. As shown *infra*, CL0P published "TORRENT MAGNET LINK" hyperlinks for many different entities that used Oracle EBS.

---

[68] *Id*.
[69] *Id*.
[70] 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.
[71] Eduard Kovacs, *Madison Square Garden Data Breach Confirmed Months After Hacker Attack*, SECURITY WEEK (March 2, 2026, 8:53 AM ET) https://www.securityweek.com/madison-square-garden-data-breach-confirmed-months-after-hacker-attack/.
[72] *Id*.

87. For context, a "magnet link" is a "hyperlink used to download data and files via peer-to-peer (P2P) networks. It functions without needing a server and includes everything a torrent client needs to obtain a particular file. . . . Magnet links trigger downloads in desktop torrent clients once a user clicks on them."[73]

88. The content, format, naming conventions, and organizational structure of the data that CL0P leaked on the Dark Web are all consistent with the Oracle E-Business Suite (EBS). For example:

a. EBS-specific table naming: The leaked files use table names and prefixes that align with well-known Oracle EBS modules (for example, Oracle Inventory tables commonly using "MTL*" naming).

b. Database table exports: The leaked data includes bulk, tabular exports (e.g., TSV files) that resemble direct database table extracts.

c. Matching table structure: The columns in the leaked files mirror the structure used in Oracle EBS tables (i.e., consistent with Oracle's published data dictionary and schemas).

d. EBS application/server layout: The directory structure of the leaked files resembles an Oracle EBS environment (e.g., the structure seen in Oracle EBS server backups and instance directories).

Defendant Anywhere Real Estate Inc.

89. Defendant, Anywhere Real Estate Inc. ("Anywhere") is a real estate firm based in New Jersey.[74]

[73] *Magnet Link*, NORD VPN, https://nordvpn.com/cybersecurity/glossary/magnet-link/ (last visited March 2, 2026).
[74] *Our Company*, ANYWHERE, https://anywhere.re/our-company/ (last visited Feb. 26, 2026).

90. As part of its business, Anywhere receives and maintains the Private Information of thousands of its current and former employees. On information and belief, the Private Information that Anywhere collects and maintains includes, *inter alia*, names, addresses, contact information, dates of birth, Social Security numbers, tax information, and financial account information.

91. In collecting and maintaining the Private Information, Anywhere agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff Tannehill and Plaintiff Nero and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, Anywhere has duties to protect the Private Information of its current and former employees and to notify them about data breaches.

92. Anywhere recognizes these duties, advertising in its "Anywhere Global Privacy Notice" that "We use technical, administrative, and physical controls in place to help protect personal information from unauthorized access, use, and disclosure."[75]

93. On information and belief, Anywhere selected Oracle as a third-party vendor and then input the Private Information of its current and former employees into the Oracle EBS system. In doing so, Anywhere disclosed the Private Information of its current and former employees to Oracle.

94. Thus far, Anywhere has admitted that:

[75] *Anywhere Global Privacy Notice*, ANYWHERE (June 12, 2025) https://privacy.anywhere.re/en/global-privacy-notice/.

a. "On November 24, 2025, Anywhere discovered a cybersecurity incident involving its Oracle E-Business Suite ('Oracle EBS') environment."[76]

b. "Upon investigation, Anywhere determined that, on August 13, 2025, an unauthorized third party had exploited a then-unknown 'zero day' Oracle software vulnerability (CVE-2025- 61882) to gain access to Anywhere's Oracle EBS environment."[77]

c. "The unauthorized third party was then able to download and export information from Anywhere's Oracle EBS environment, including certain information about franchisees and brokers."[78]

d. "Anywhere discovered that some personal information about current and former employees had also been subject to unauthorized access, as a result of this incident. The impacted personal information includes name, address, contact information, date of birth, Social Security number, and basic job details, such as location and hire date[.]"[79]

95. Thus far, Anywhere has stated that 17,429 of its current and former employees were exposed.[80]

[76] *Notice of a Breach of Security of a System*, NEW HAMPSHIRE ATTY GEN (Feb. 6, 2026) https://mm.nh.gov/files/uploads/doj/remote-docs/anywhere-real-estate-20260206.pdf.
[77] *Id*.
[78] *Id*.
[79] *Id*.
[80] *Data Breach Notifications*, MAINE ATTY GEN (Jan. 30, 2026) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/c286e6aa-68a7-47e6-8847-4ef8a9cba713.html.

96. On or around November 21, 2025, CL0P published information about Anywhere on its Dark Web leak site (a screenshot is provided below).[81]



97. Based on these facts, CL0P has already published the Private Information that CL0P obtained from Anywhere during the Data Breach.

98. And yet, Anywhere waited until January 30, 2026, before providing a notification about the Data Breach.[82] Thus, Anywhere kept Plaintiff Tannehill and Plaintiff Nero and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

[81] *ANYWHERE.RE*, RANSOM LOOK (Nov. 21, 2025) https://www.ransomlook.io/screenshots/clop/ANYWHERERE.png.
[82] *Notice of a Breach of Security of a System*, NEW HAMPSHIRE ATTY GEN (Feb. 6, 2026) https://mm.nh.gov/files/uploads/doj/remote-docs/anywhere-real-estate-20260206.pdf.

99. Notably, Anywhere acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "[w]e recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies."[83]

100. Anywhere breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

101. Through its breaches, Anywhere injured Plaintiff Tannehill and Plaintiff Nero and relevant Class Members.

Defendant Cox Enterprises, Inc.

102. Defendant, Cox Enterprises, Inc. ("Cox") is a private firm focused on telecommunications, automotive, and media.[84]

103. As part of its business, Cox receives and maintains the Private Information of thousands of its current and former employees and contractors. On information and belief, the Private Information that Cox collects and maintains includes, *inter alia*, names, contact information, Social Security numbers, taxpayer identification numbers, government ID numbers, passport numbers, state ID card numbers, and financial account information.[85]

---

[83] *Id*.
[84] *Home Page*, COX ENTERPRISES, https://www.coxenterprises.com/ (last visited Feb. 26, 2026).
[85] *See, e.g., Data Security Breach Reports*, TEX ATTY GEN (Nov. 21, 2025) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

104. In collecting and maintaining the Private Information, Cox agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs Massengill and Issac and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, Cox has duties to protect the Private Information of its current and former employees and contractors and to notify them about data breaches.

105. Cox recognizes these duties, advertising in its "Applicant Privacy Notice" that:

a. "The Company is committed to protecting Applicant Personal Information from unauthorized disclosure, use, acquisition, or loss."[86]

b. "We employ reasonable and appropriate technical, physical, and administrative controls to safeguard our information systems that contain Applicant Personal Information."[87]

c. "We also impose controls and contractual obligations on third parties that have access to Applicant Information."[88]

106. On information and belief, Cox selected Oracle as a third-party vendor and then input the Private Information of its current and former employees and contractors into the Oracle EBS system. In doing so, Cox disclosed the Private Information of its current and former employees and contractors to Oracle.

107. Thus far, Cox has admitted that:

[86] *Applicant Privacy Policy*, COX ENTERPRISES, https://www.coxenterprises.com/applicant-privacy-policy (last visited Feb. 26, 2026).
[87] *Id*.
[88] *Id*.

a. "On September 29, 2025, we became aware of suspicious activity involving Oracle's E-Business Suite, which is a platform we use for some of our back-office business operations."[89]

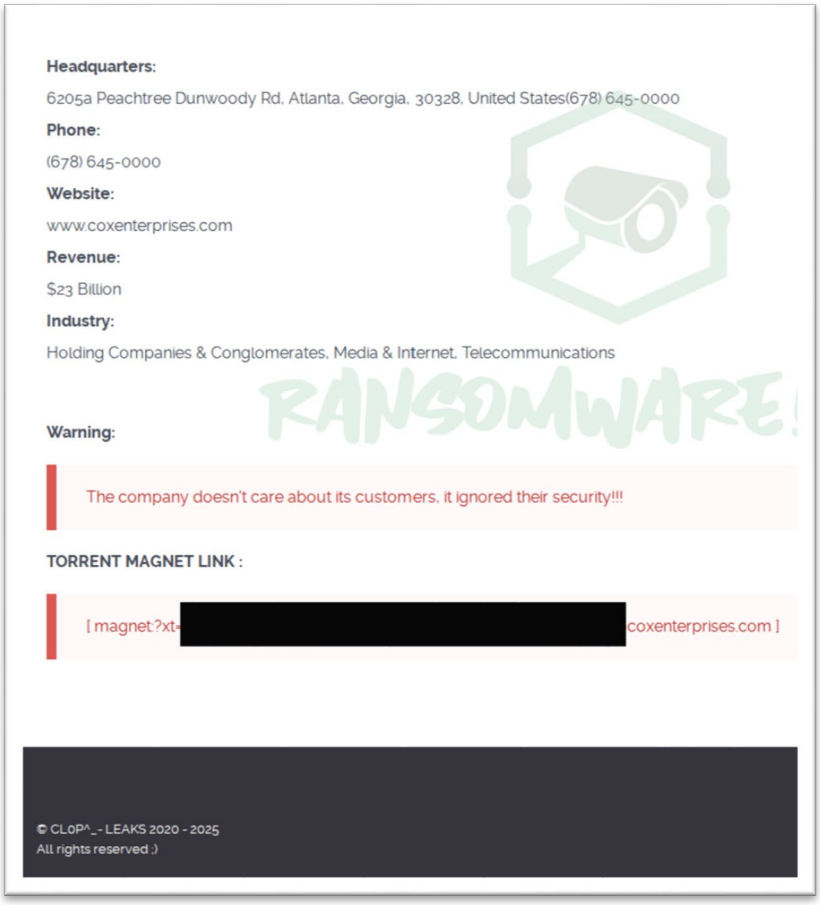
b. "We learned the suspicious activity was the result of cybercriminals taking advantage of a previously unknown security flaw (called a 'zero-day' vulnerability) in Oracle's E-Business Suite between Aug. 9-14, 2025."[90]

c. "Unfortunately, this issue affected many companies that use Oracle's systems, including Cox."[91]

108. Thus far, Cox has stated that 9,479 of its current and former employees and contractors were exposed.[92]

109. But on or around October 27, 2025, CL0P published information about Cox on its Dark Web leak site.[93] Therein, CL0P published a "TORRENT MAGNET LINK" which, on information and belief, leaked the Private Information that Cox had disclosed to Oracle.[94] A screenshot is provided below (with a portion of the TORRENT MAGNET LINK redacted to prevent further dissemination of the published Private Information).[95]

[89] *Notice of Data Breach*, MAINE ATTY GEN (Nov. 20, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/314b7585-15e4-4574-b102-6593275436d2.html.
[90] *Id*.
[91] *Id*.
[92] *Id*.
[93] *Cox*, RANSOMWARE LIVE (Oct. 27, 2025) https://www.ransomware.live/id/Q09YRU5URVJQUklTRVMuQ09NQGNsb3A.
[94] *Id*.
[95] *Id*.



110. Thereafter, CL0P published on its Dark Web leak site approximately 1.520 tebibytes of data that appear to originate from Cox.

111. Based on these facts, CL0P has already published the Private Information that CL0P obtained from Cox during the Data Breach.

112. And yet, Cox waited until November 20, 2025, before providing a notification about the Data Breach.[96] Cox kept Plaintiffs Massengill and Issac and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

[96] *Id.*

113. Notably, Cox acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "we also encourage you to review your credit reports and financial statements."[97]

114. Cox breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

115. Through its breaches, Cox injured Plaintiffs Massengill and Issac and relevant Class Members.

GlobalLogic Inc.

116. GlobalLogic Inc. ("GlobalLogic") is a global engineering firm based in Santa Clara, California.[98]

117. GlobalLogic is not a named Defendant, and Plaintiffs do not assert any claims against GlobalLogic.

118. As part of its business, GlobalLogic receives and maintains the Private Information of thousands of its current and former employees.

119. Thus far, GlobalLogic has admitted that:

a. "Oracle issued a security advisory on October 4, 2025, about a previously unknown zero-day exploit. GlobalLogic uses Oracle E-Business Suite, a

[97] *Id*.
[98] *Locations*, GLOBALLOGIC, https://www.globallogic.com/about/locations/ (last visited Feb. 26, 2026).

collection of applications, to manage core business functions such as finance, HR, accounts payable and receivable."[99]

b. "As soon as we learned of the vulnerability, GlobalLogic immediately investigated and determined that it had been exploited within our instance of Oracle."[100]

c. "GlobalLogic's investigation identified access to Oracle and exfiltration on October 9, 2025."[101]

d. "The investigation has identified the earliest date of threat actor activity as July 10, 2025, with the most recent activity occurring on August 20, 2025."[102]

e. "What Information was Involved? The personal information involved in this incident was from our Oracle platform, which includes HR information for current and former personnel. That information includes personal information collected as part of Human Resources, and could involve the following information of yours: name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, internal GlobalLogic employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."[103]

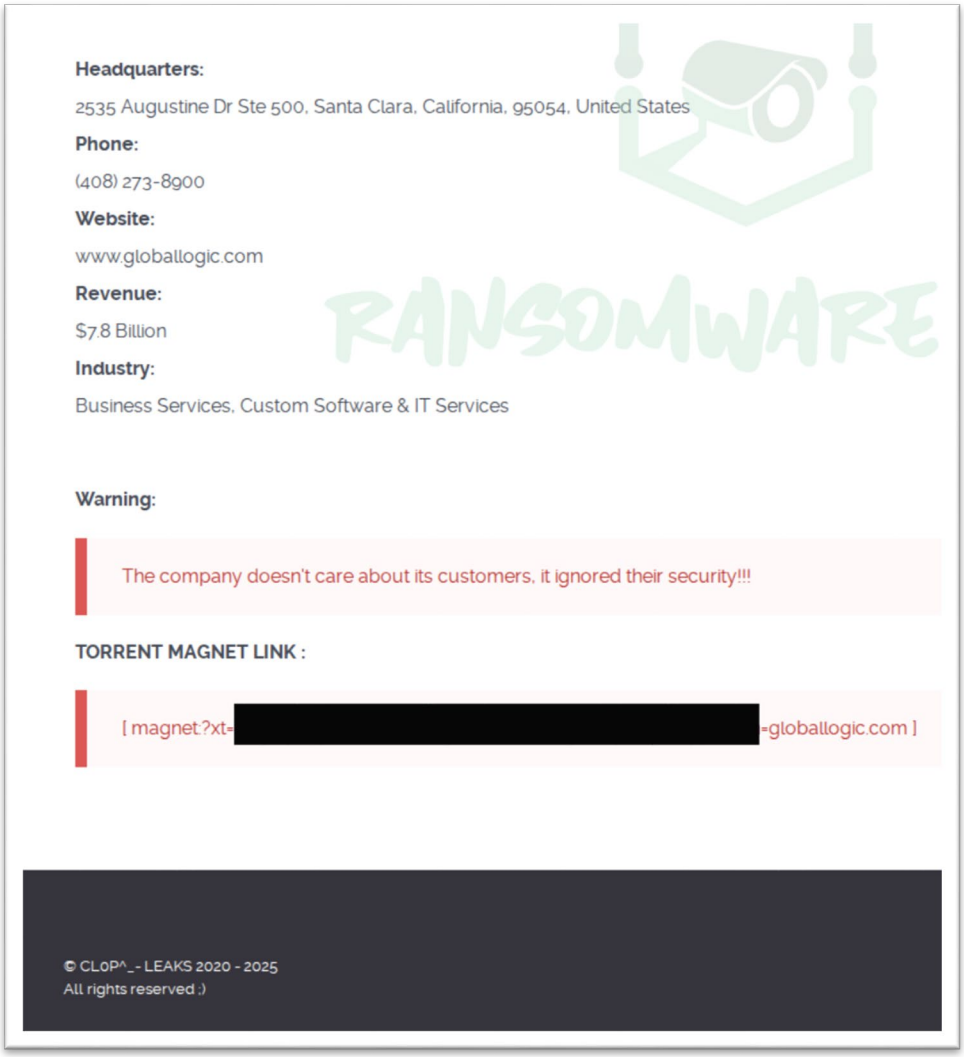
---

[99] *Data Breach Notifications*, MAINE ATTY GEN (Nov. 7, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a69e0001-a0f8-46d9-a49d-cb01159afec2.html.
[100] *Id*.
[101] *Id*.
[102] *Id*.
[103] *Id*.

120. Thus far, GlobalLogic has stated that 10,471 of its current and former employees were exposed.[104]

121. On or around November 13, 2025, CL0P published information about GlobalLogic on its Dark Web leak site.[105] Therein, CL0P published a "TORRENT MAGNET LINK" which, on information and belief, leaked the Private Information that GlobalLogic had disclosed to Oracle.[106] A screenshot is provided below (with a portion of the TORRENT MAGNET LINK redacted to prevent further dissemination of the published Private Information).[107]

[104] *Id*.
[105] *GLOBALLOGIC.COM*, RANSOMWARE LIVE (Nov. 13, 2025) https://www.ransomware.live/id/R0xPQkFMTE9HSUMuQ09NQGNsb3A.
[106] *Id*.
[107] *Id*.



122. Based on these facts, CL0P has already published the Private Information that CL0P obtained from GlobalLogic during the Data Breach.

123. Notably, GlobalLogic acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for

suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft."[108]

Defendant LKQ Corporation

124. Defendant, LKQ Corporation ("LKQ") is a global automotive products and services firm.[109]

125. As part of its business, LKQ receives and maintains the Private Information of thousands of its current and former employees and/or contractors. On information and belief, the Private Information that LKQ collects and maintains includes, *inter alia*, names and Social Security numbers.

126. In collecting and maintaining the Private Information, LKQ agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff Reynolds and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, LKQ has duties to protect the Private Information of its current and former employees and/or contractors and to notify them about data breaches.

127. LKQ recognizes these duties, advertising in its "Privacy Statement" that:

a. "HOW WE PROTECT PERSONAL DATA. We maintain administrative, technical and physical safeguards, consistent with legal requirements where the personal data was obtained, designed to protect against unlawful or unauthorized destruction, loss, alteration, use or disclosure of, or access to, the personal data provided to us through the Services."[110]

[108] *Id*.
[109] *Home Page*, LKQ, https://lkqcorp.com/ (last visited Feb. 26, 2026).
[110] *Privacy Statement*, LKQ (Dec. 20, 2022) https://lkqcorp.com/privacy/.

128. On information and belief, LKQ selected Oracle as a third-party vendor and then input the Private Information of its current and former employees and/or contractors into the Oracle EBS system. In doing so, LKQ disclosed the Private Information of its current and former employees and/or contractors to Oracle.

129. Thus far, LKQ has admitted that:

a. "Recently, Oracle announced a number of security vulnerabilities, including a previously unknown vulnerability in its E-Business Suite application, which is used by LKQ and many other organizations worldwide. In early October, our security team became aware of a third party exploiting these vulnerabilities."[111]

b. "We completed this process December 1, 2025, and are providing you notice because our records indicate that you are a sole proprietor supplier of LKQ and your Employer Identification Number or Social Security number was impacted."[112]

130. Thus far, LKQ has stated that 9,070 of its current and former employees and/or contractors were exposed.[113]

131. On or around October 27, 2025, CL0P published information about LKQ on its Dark Web leak site.[114] Therein, CL0P published three "TORRENT MAGNET LINK" which, on

[111] *Data Breach Notification*, MAINE ATTY GEN (Dec. 15, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0f46ebfd-5508-426d-88f9-3ad07e6ef483.html.
[112] *Id*.
[113] *Id*.
[114] *LKQCORP.COM*, RANSOMWARE LIVE (Oct. 27, 2025) https://www.ransomware.live/id/TEtRQ09SUC5DT01AY2xvcA.

information and belief, leaked the Private Information that LKQ had disclosed to Oracle.[115] A screenshot is provided below (with portions of the TORRENT links redacted).



132. Based on these facts, CL0P has already published the Private Information that CL0P obtained from LKQ during the Data Breach.

[115] *Id.*

133. And yet, LKQ waited until December 15, 2025, before providing a notification about the Data Breach.[116] LKQ kept Plaintiff Reynolds and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

134. Notably, LKQ acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity."[117]

135. LKQ breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

136. Through its breaches, LKQ injured Plaintiff Reynolds and relevant Class Members.

Defendant Madison Square Garden Entertainment Corp.

137. Defendant, Madison Square Garden Entertainment Corp. ("MSG") is a live entertainment company that operates a "portfolio of iconic venues: New York's Madison Square Garden, the Infosys Theater at Madison Square Garden, Radio City Music Hall, and Beacon Theatre; and The Chicago Theatre[.]"[118]

---

[116] *Id*.
[117] *Id*.
[118] *Our Company*, MADISON SQUARE GARDEN ENTERTAINMENT, https://www.msgentertainment.com/our-company/ (last visited March 2, 2026).

138. As part of its business, MSG receives and maintains the Private Information of thousands of its current and former employees. On information and belief, the Private Information that MSG collects and maintains includes, *inter alia*, names, addresses, contact information, Social Security numbers, dates of birth, tax information, and financial account information.

139. In collecting and maintaining the Private Information, MSG agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff Alvarado and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, MSG has duties to protect the Private Information of its current and former employees and to notify them about data breaches.

140. MSG recognizes these duties, advertising in its "Privacy Policy" that:

a. "This Madison Square Garden Privacy Policy ('Policy') describes the information that the Madison Square Garden Family ('collectively, the 'MSG Family' defined below) collects, how we use it, and when and with whom we may disclose it."[119]

b. "For purposes of this Policy, the terms 'MSG Family,' 'we,' 'us,' and 'our' include, without limitation, three groups of entities . . . Madison Square Garden Entertainment Corp. and each of its respective subsidiaries, divisions, affiliated entities and business units, as may change from time to time[.]"[120]

c. "We have implemented administrative, technical, and physical security measures to protect against the loss, misuse and/or alteration of your

[119] *Privacy Policy*, MADISON SQUARE GARDEN ENTERTAINMENT (Jan. 9, 2025) https://www.msgentertainment.com/privacy/.
[120] *Id*.

information. These safeguards vary based on the sensitivity of the information that we collect and store."[121]

d. "We generally retain personal data for so long as it may be relevant to the purposes above. In determining how long to retain information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the information, the purposes for which we process the information, applicable legal requirements, and our legitimate interests."[122]

141. On information and belief, MSG selected Oracle as a third-party vendor and then input the Private Information of its current and former employees into the Oracle EBS system. In doing so, MSG disclosed the Private Information of its current and former employees to Oracle.

142. Thus far, MSG has admitted that:

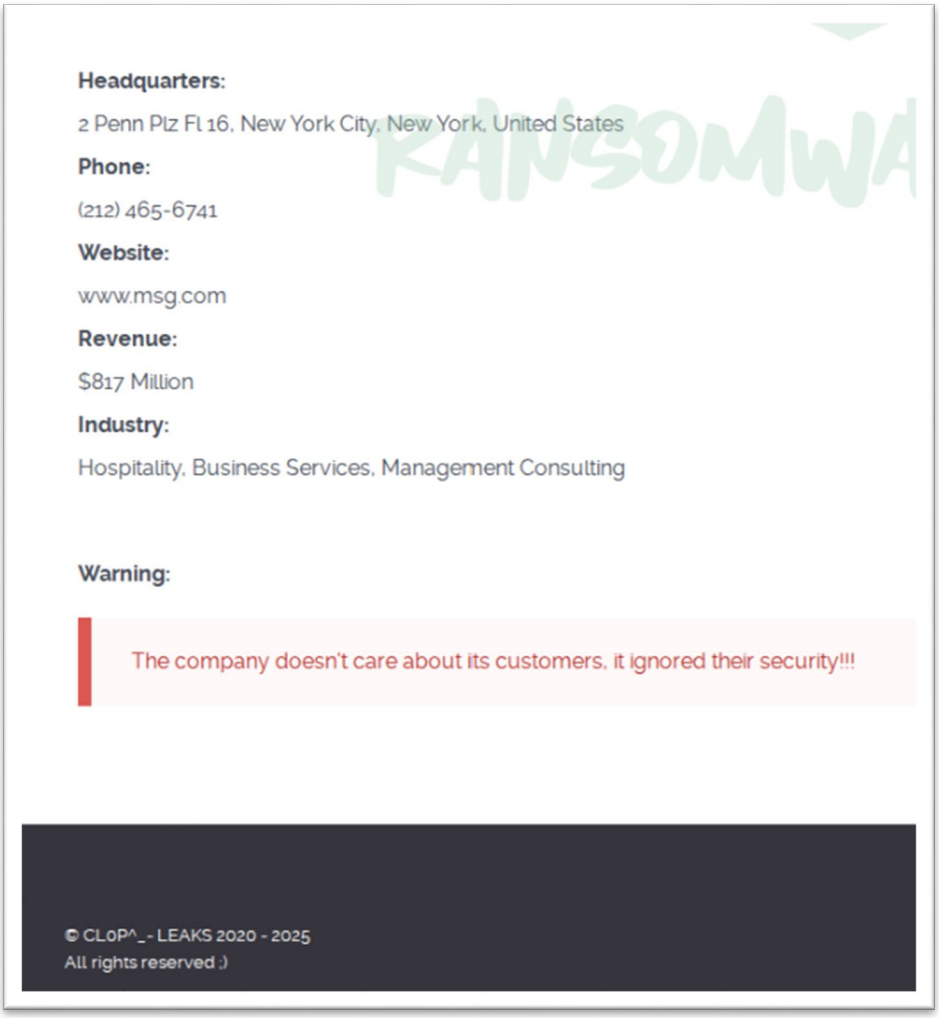
a. "The Oracle eBusiness Suite, hosted and managed for Madison Square Garden Entertainment Corp. ('Madison Square Garden') by a vendor, is used for certain workforce and financial operations. Oracle notified its customers that a previously undisclosed condition in the application had been exploited by an unauthorized person to gain access to data from the application. There are reports that this occurred at over 100 companies."[123]

b. "Madison Square Garden reviewed the files and in December 2025, determined that a file containing the names and Social Security numbers of

[121] *Id*.
[122] *Id*.
[123] *Data Breach Notifications*, MAINE ATTY GEN (Feb. 26, 2026) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/44a0bea6-9a88-49c9-81ed-3b6f388f9f8b.html.

11 Maine residents was involved. The files were part of business records related to hiring or payments made to individuals."[124]

143. On or around November 21, 2025, CL0P published information about MSG on its Dark Web leak site (a screenshot is provided below).[125]



144. Thereafter, CL0P published on its Dark Web leak site approximately 196.65 gibibytes of data including 92,208 Social Security numbers that appear to originate from MSG.

[124] *Id.*
[125] *MSG.COM*, RANSOMWARE LIVE (Nov. 21, 2025) https://www.ransomware.live/id/TVNHLkNPTUBjbG9w.

145. Based on these facts, CL0P has already published the Private Information that CL0P obtained from MSG during the Data Breach.

146. And yet, MSG waited until February 26, 2026, before providing a notification about the Data Breach.[126] MSG kept Plaintiff Alvarado and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

147. Notably, MSG acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity."[127]

148. MSG breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

149. Through its breaches, MSG injured Plaintiffs Alvarado and Liranzo and relevant Class Members.

Defendant Parexel International, LLC

150. Defendant, Parexel International, LLC ("Parexel") is a global clinical research organization.[128]

[126] *Id*.
[127] *Id*.
[128] *Home Page*, PAREXEL, https://www.parexel.com/ (last visited Feb. 26, 2026).

151. As part of its business, Parexel receives and maintains the Private Information of thousands of its current and former employees. On information and belief, the Private Information that Parexel collects and maintains includes, *inter alia*, names, dates of birth, financial account numbers, payment card numbers, Social Security numbers, and national ID numbers.

152. In collecting and maintaining the Private Information, Parexel agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs Youmell, Trempus, O'Keeffe, and Naulty and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, Parexel has duties to protect the Private Information of its current and former employees and to notify them about data breaches.

153. Parexel recognizes these duties, advertising in its "Privacy Policy" that:

a. "Information Security. Parexel maintains a reasonable level of physical, electronic and managerial procedures in order to protect the information that it collects from its website. This includes maintaining computer equipment, networks, programs and documentation to a common standard and restricting access to equipment and information to appropriate staff."[129]

154. On information and belief, Parexel selected Oracle as a third-party vendor and then input the Private Information of its current and former employees into the Oracle EBS system. In doing so, Parexel disclosed the Private Information of its current and former employees to Oracle.

155. Thus far, Parexel has admitted that:

[129] *Privacy Policy*, PAREXEL (Dec. 2025) https://www.parexel.com/about-us/trust-and-privacy/privacy-policy.

a. "On October 4, 2025, we detected suspicious activity impacting a portion of our Oracle OCI E-Business Suite ('Oracle EBS') environment hosted by Oracle and immediately engaged third-party cybersecurity experts to investigate."[130]

b. "Our investigation has confirmed the activity stemmed from a zero-day exploit impacting Oracle's cloud infrastructure that was announced by Oracle on October 5, 2025."[131]

c. "The files may have contained your name, date of birth, financial account number and/or payment card number (without CVV), social security and/or national ID number provided to Parexel in connection with your employment."[132]

156. Based on these facts, CL0P has already published the Private Information that CL0P obtained from Parexel during the Data Breach.

157. And yet, Parexel waited until December 17, 2025, before providing a notification about the Data Breach.[133] Parexel kept Plaintiffs Youmell, Trempus, O'Keeffe, and Naulty and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

158. Notably, Parexel acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "We recommend that

[130] *Data Breach Notification*, MAINE ATTY GEN (Dec. 17, 2026) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/93eaad97-1cd2-4f3e-9e42-513cfdad3d2d.html.
[131] *Id*.
[132] *Id*.
[133] *Id*.

you monitor your credit reports for any activity you do not recognize" and "We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider."[134]

159. Parexel breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

160. Through its breaches, Parexel injured Plaintiffs Youmell, Trempus, O'Keeffe, and Naulty and relevant Class Members.

Defendant The Research Foundation for The State University of New York

161. Defendant, The Research Foundation for The State University of New York ("RF SUNY") is a non-profit educational corporation that administers research activity for The State University of New York.[135]

162. As part of its business, RF SUNY receives and maintains the Private Information of thousands of its current and former employees. On information and belief, the Private Information that RF SUNY collects and maintains includes, *inter alia*, names and Social Security numbers.

163. In collecting and maintaining the Private Information, RF SUNY agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all,

[134] *Id*.
[135] *Non-Profit Tax-Exempt (Form 990)*, RF SUNY, https://www.rfsuny.org/About-Us/Reports--Publications/Non-Profit-Tax-Exempt-IRS-Form-990/ (last visited Feb. 26, 2026).

Plaintiff Yao and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, RF SUNY has duties to protect the Private Information of its current and former employees and to notify them about data breaches.

164. RF SUNY recognizes these duties, advertising in its "Privacy Policy" that:

a. "The RF recognizes the need to appropriately manage and protect personal information that you share with us. This privacy policy reflects our commitment to treating your information with care."[136]

165. On information and belief, RF SUNY selected Oracle as a third-party vendor and then input the Private Information of its current and former employees into the Oracle EBS system. In doing so, RF SUNY disclosed the Private Information of its current and former employees to Oracle.

166. Thus far, RF SUNY has admitted that:

a. "On October 10, 2025, RF SUNY learned that unauthorized parties exploited a zero-day vulnerability in Oracle's E-Business Suite application, which RF SUNY uses to maintain business information, including human resources and benefits-related information."[137]

b. "Through our investigation, on October 13, 2025, RF SUNY determined that the vulnerability in the Oracle's E-Business Suite application allowed unauthorized parties to access and acquire files stored in the application between August 9 and 11, 2025."[138]

[136] *Privacy Policy*, RF SUNY, https://www.rfsuny.org/privacy-policy--terms-of-use/ (last visited Feb. 26, 2026).
[137] *See* Exhibit A (data breach notice of Richard Yao).
[138] *Id*.

c. "As part of the ongoing investigation, RF SUNY worked diligently to identify the files that were subject to unauthorized access / acquisition as a result of the vulnerability in Oracle's E-Business Suite application. On November 26, 2025, RF SUNY determined one or more files contained your name and Social Security number."[139]

167. On or around November 21, 2025, CL0P published information about RF SUNY on its Dark Web leak site.[140] Therein, CL0P published a "TORRENT MAGNET LINK" which, on information and belief, leaked the Private Information that RF SUNY had disclosed to Oracle.[141] A screenshot is provided below (with a portion of the TORRENT MAGNET LINK redacted to prevent further dissemination of the published Private Information).

[139] *Id*.
[140] *RFSUNY.ORG*, RANSOMWARE LIVE (Nov. 21, 2025) https://www.ransomware.live/id/UkZTVU5ZLk9SR0BjbG9w.
[141] *Id*.



168. Thereafter, CL0P published on its Dark Web leak site approximately 330.50 gibibytes of data which included approximately 144,600 Social Security numbers that appear to originate from RF SUNY.

169. Based on these facts, CL0P has already published the Private Information that CL0P obtained from RF SUNY during the Data Breach.

170. And yet, RF SUNY waited until January 29, 2026, before providing a notification about the Data Breach.[142] RF SUNY kept Plaintiff Yao and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

[142] *Id.*

171. RF SUNY breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

172. Through its breaches, RF SUNY injured Plaintiff Yao and relevant Class Members.

Defendant Trustees of Dartmouth College

173. Defendant, Trustees of Dartmouth College d/b/a Dartmouth College ("Dartmouth") is an educational institution in Hanover, New Hampshire.[143]

174. As part of its business, Dartmouth receives and maintains the Private Information of thousands of its current and former students and employees. On information and belief, the Private Information that Dartmouth collects and maintains includes, *inter alia*, names, Social Security numbers, and financial account information.

175. In collecting and maintaining the Private Information, Dartmouth agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs Ross and Mabey and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, Dartmouth has duties to protect the Private Information of its current and former students and employees and to notify them about data breaches.

[143] *Tax Compliance*, DARTMOUTH, https://www.dartmouth.edu/finance/financial-management/tax_compliance/index.php (last visited Feb. 26, 2026).

176. Dartmouth recognizes these duties, advertising in its "Dartmouth Information Security Policy" that:

a. "The goal of Dartmouth's Information Security Policy is to protect the institution's confidential information."[144]

b. "To this end, Dartmouth has adopted a comprehensive security policy for the processing, sharing, and storage of information, including electronic, paper, and other media."[145]

c. "All Dartmouth offices and employees (faculty and staff) must comply with institutional information security policy, and apply the standards and controls that are applicable to the Dartmouth information they manage and use."[146]

d. "Data classified as level 3 are data classified as strictly confidential, requiring the highest level of sensitivity. This includes FERPA data, personally identifiable information (PII), personal health information (PHI), credit card information (PCI), among others."[147]

177. On information and belief, Dartmouth selected Oracle as a third-party vendor and then input the Private Information of its current and former students and employees into the Oracle EBS system. In doing so, Dartmouth disclosed the Private Information of its current and former students and employees to Oracle.

---

[144] *Dartmouth Information Security Policy*, DARTMOUTH, https://policies.dartmouth.edu/policy/dartmouth-information-security-policy (last visited Feb. 26, 2026).
[145] *Id*.
[146] *Id*.
[147] *Id*.

178. Thus far, Dartmouth has admitted that:

a. "We recently completed an investigation of a data security incident that involved our Oracle eBusiness Suite ('EBS') software. Dartmouth, like many institutions and entities around the world, uses Oracle EBS to help manage our operations."[148]

b. "As has been reported in the press, the Oracle EBS software experienced a 'zero-day' vulnerability, which is an unknown vulnerability, that allowed an unauthorized actor to take data, from many of Oracle's EBS customers' environments, including Dartmouth's."[149]

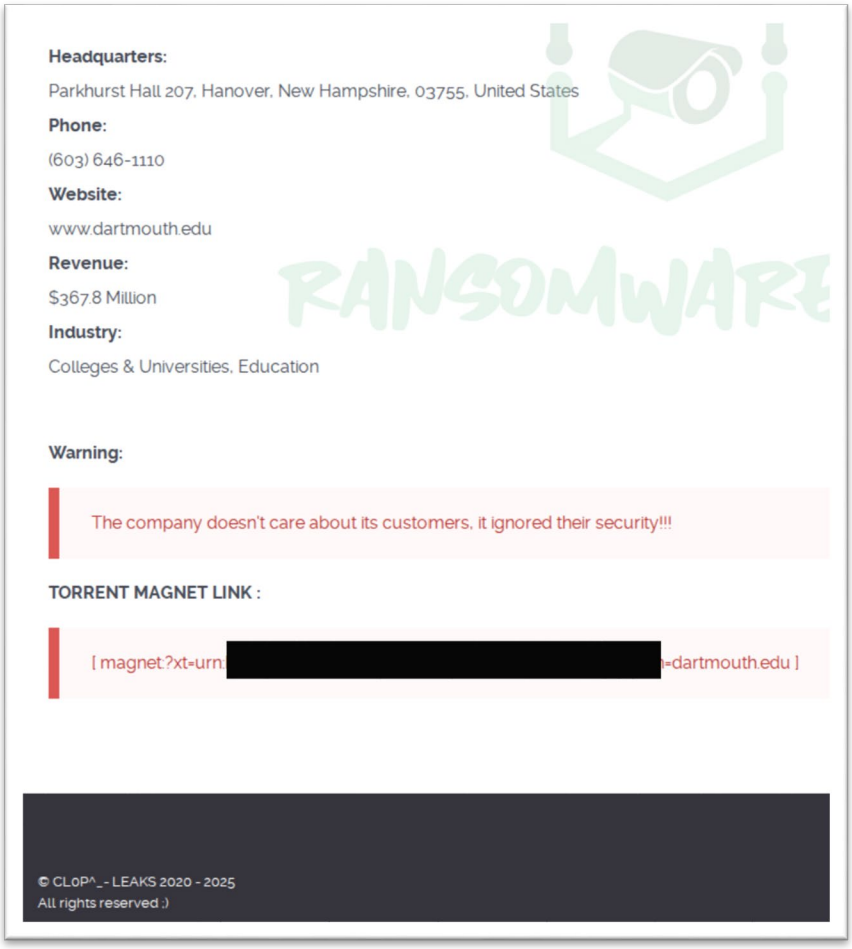
c. "Through the investigation, we determined that an unauthorized actor took certain files between August 9, 2025, and August 12, 2025."[150]

d. "We reviewed the files and on October 30, 2025, identified one or more that contained your name and Social Security number."[151]

179. On or around November 13, 2025, CL0P published information about Dartmouth on its Dark Web leak site.[152] Therein, CL0P published a "TORRENT MAGNET LINK" which, on information and belief, leaked the Private Information that Dartmouth had disclosed to Oracle.[153] A screenshot is provided below (with a portion of the TORRENT MAGNET LINK redacted to prevent further dissemination of the published Private Information).

---

[148] *Data Breach Notifications*, MAINE ATTY GEN (Nov. 24, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ce67c791-f72f-415a-91fa-b7ba563ca747.html.
[149] *Id*.
[150] *Id*.
[151] *Id*.
[152] *DARTMOUTH.EDU*, RANSOMWARE LIVE (Nov. 13, 2025) https://www.ransomware.live/id/REFSVE1PVVRILkVEVUBjbG9w.
[153] *Id*.



180. Thereafter, CL0P published on its Dark Web leak site approximately 210.78 gibibytes of data that include Social Security numbers and appear to originate from Dartmouth.

181. Based on these facts, CL0P has already published the Private Information that CL0P obtained from Dartmouth during the Data Breach.

182. And yet, Dartmouth waited until November 24, 2025, before providing a notification about the Data Breach.[154] Dartmouth kept Plaintiffs Ross and Mabey and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

[154] *Id.*

183. Notably, Dartmouth acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months."[155]

184. Dartmouth breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

185. Through its breaches, Dartmouth injured Plaintiffs Ross and Mabey and relevant Class Members.

Defendant University of Pennsylvania

186. Defendant, The Trustees of the University of Pennsylvania d/b/a University of Pennsylvania ("UPenn") is an educational institution based in Philadelphia, Pennsylvania.[156]

187. As part of its business, UPenn receives and maintains the Private Information of thousands of its current and former employees and students. On information and belief, the Private Information that UPenn collects and maintains includes, *inter alia*, names, addresses, Social Security numbers, financial account numbers (e.g., account numbers, credit card numbers, debit card numbers).

---

[155] *Data Breach Notifications*, MAINE ATTY GEN (Nov. 24, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ce67c791-f72f-415a-91fa-b7ba563ca747.html.
[156] *Home Page*, PENN, https://www.upenn.edu/ (last visited Feb. 26, 2026).

188. In collecting and maintaining the Private Information, UPenn agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff Gilula and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, UPenn has duties to protect the Private Information of its current and former employees and students and to notify them about data breaches.

189. UPenn recognizes these duties, advertising in its "Privacy Policy" that:

a. "We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization."[157]

190. On information and belief, UPenn selected Oracle as a third-party vendor and then input the Private Information of its current and former employees and students into the Oracle EBS system. In doing so, UPenn disclosed the Private Information of its current and former employees and students to Oracle.

191. Thus far, UPenn has admitted that:

a. "Penn uses a third-party software tool called Oracle E-Business Suite ('Oracle EBS') from Oracle, a third-party technology provider."[158]

b. "Oracle EBS is a financial application used to process supplier payments, reimbursements, general ledger entries, and to conduct other University business."[159]

---

[157] *Privacy Policy*, PENN, https://www.upenn.edu/about/privacy-policy (last visited Feb. 26, 2026).
[158] *Data Breach Notifications*, MAINE ATTY GEN (Dec. 1, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/6de24e56-1806-4f42-853e-6c505ee1427f.html.
[159] *Id*.

c. "Oracle recently announced a previously unknown security vulnerability that could allow unauthorized access to Oracle EBS and data stored in it."[160]

d. "In the course of Penn's own investigation, we discovered that some data from Penn's Oracle EBS had been obtained without authorization."[161]

e. "On November 11, 2025, Penn determined that your personal information was among the information obtained from Oracle EBS."[162]

192. UPenn has confirmed that the types of Private Information exposed include, at least, names, addresses, Social Security numbers, financial account numbers (e.g., account numbers, credit card numbers, debit card numbers).[163]

193. Based on these facts, CL0P has already published the Private Information that CL0P obtained from UPenn during the Data Breach.

194. And yet, UPenn waited until December 1, 2025, before providing a notification about the Data Breach.[164] UPenn kept Plaintiff Gilula and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

195. Notably, UPenn acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "we encourage you to remain vigilant[.]"[165]

196. UPenn breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure

---

[160] *Id*.
[161] *Id*.
[162] *Id*.
[163] *Data Breach Security Reports*, TEXAS ATTY GEN (Dec. 3, 2025) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.
[164] *Id*.
[165] *Id*.

that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

197. Through its breaches, UPenn injured Plaintiff Gilula and relevant Class Members.

Defendant University of Phoenix

198. Defendant, University of Phoenix, Inc. (the "University of Phoenix") is a university based in Phoenix, Arizona, and offers extensive online classes.[166]

199. As part of its business, the University of Phoenix receives and maintains the Private Information of thousands of its current and former students and employees. On information and belief, the Private Information that the University of Phoenix collects and maintains includes, *inter alia*, names, dates of birth, Social Security numbers, and financial account information.

200. In collecting and maintaining the Private Information, the University of Phoenix agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs Mosby, Ranson, Pointer, Vega, and Wyche and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, the University of Phoenix has duties to protect the Private Information of its current and former students and employees and to notify them about data breaches.

201. The University of Phoenix recognizes these duties, advertising in its "Privacy Policy" that:

a. "While the Personal Information we collect varies (as explained above) depending upon the nature of the Services provided or used and our

[166] *Home Page*, UNIV. PHOENIX, https://www.phoenix.edu (last visited March 5, 2026).

interactions with individuals, generally, we may collect the following categories of Personal Information: Name, contact information, and other identifiers: real name, alias, postal address, telephone number(s), unique personal identifier, online identifier, email address, account name, signature, or other similar identifiers . . . Financial information: bank account number, credit card number, debit card number, federal tax filing information, or other financial information . . . Medical information, disability, and health insurance information: to support specific programmatic or regulatory requirements or service requests . . . Demographic information: characteristics such as race, ethnicity, gender, age, religion, national origin, citizenship or immigration status, and marital status . . . Government identification: Social Security, driver's license, state ID, and passport numbers and/or corresponding identification document(s)[.]"[167]

b. "We have implemented security measures to protect against the loss, misuse, and alteration of the Personal Information under our control."[168]

202. The separate "University of Phoenix Policy on Applicant Privacy" advertises that:

a. "Generally, we may collect the following categories of Personal Information about you and use it for the purposes listed below during the application process: Name, Contact Information, and Other Identifiers: Real name, alias, postal address, telephone number(s), internet protocol (IP)

[167] *University of Phoenix Privacy Policy*, UNIV. PHOENIX (Nov. 10, 2025) https://www.phoenix.edu/copyright-legal/privacy-policy.html.
[168] *Id*.

address, email address, social security number, driver's license number, passport number, or other similar identifiers."[169]

b. "We may also disclose Personal Information to third-party service providers related to recruitment, employment, and suitability screening processes as well as those that support our Human Resources functions. These third-party service providers may collect or have access to information only for the purpose of performing services specified in the applicable service contract, and we require these providers to undertake reasonable security measures to protect your data."[170]

c. "How Long We Retain Information. For each category of Personal Information collected, we only retain such Personal Information for as long as necessary to fulfill the purposes outlined in this policy and as otherwise needed to address tax, corporate, compliance, litigation, and other legal rights and obligations."[171]

d. "Safeguarding the Information We Collect. We have implemented security measures to protect against the loss, misuse, and alteration of the Personal Information under our control."[172]

203. On information and belief, the University of Phoenix selected Oracle as a third-party vendor and then input the Private Information of its current and former students and

[169] *University of Phoenix Policy on Applicant Privacy*, UNIV. PHOENIX (Oct. 28, 2025) https://www.phoenix.edu/copyright-legal/applicant-privacy.html.
[170] *Id*.
[171] *Id*.
[172] *Id*.

employees into the Oracle EBS system. In doing so, the University of Phoenix disclosed the Private Information of its current and former students and employees to Oracle.

204. Thus far, the University of Phoenix has admitted that:

a. "On November 21, 2025, the University of Phoenix learned that an Oracle E-Business Suite ('Oracle EBS') software vulnerability may have resulted in a cybersecurity incident."[173]

b. "On November 24, 2025, the University of Phoenix determined that, like many other organizations, including other academic institutions, 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. This exfiltration occurred between August 13 and 22, 2025."[174]

c. "The incident may have involved names, dates of birth, Social Security numbers, and bank account and routing numbers[.]"[175]

205. Thus far, the University of Phoenix has stated that 3,489,274 of its current and former students and employees were exposed.[176]

206. Based on these facts, CL0P has already published the Private Information that CL0P obtained from the University of Phoenix during the Data Breach.

---

[173] *Data Breach Notifications*, MAINE ATTY GEN (Dec. 22, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/422db005-448f-4772-afc6-07dabfa169a8.html.
[174] *Id.*
[175] *Id.*
[176] *Id.*

207. And yet, the University of Phoenix waited until December 22, 2025, before providing a notification about the Data Breach.[177] The University of Phoenix kept Plaintiffs Mosby, Ranson, Pointer, Vega, Clark, and Wyche and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

208. Notably, the University of Phoenix acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "we recommend that you remain vigilant by reviewing your account statements and credit reports closely."[178]

209. The University of Phoenix breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches, failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

210. Through its breaches, The University of Phoenix injured Plaintiffs Mosby, Ranson, Pointer, Vega, Clark, and Wyche and relevant Class Members.

Defendant WP Company LLC

211. Defendant, WP Company LLC d/b/a The Washington Post (the "Washington Post") is a newspaper based in Washington, DC.[179]

[177] *Id*.
[178] *Id*.
[179] *Home Page*, THE WASHINGTON POST, https://www.washingtonpost.com/ (last visited Feb. 26, 2026).

212. As part of its business, the Washington Post receives and maintains the Private Information of thousands of its current and former employees and contractors. On information and belief, the Private Information that the Washington Post collects and maintains includes, *inter alia*, names, bank account numbers (including routing numbers), Social Security numbers, and tax ID numbers.

213. In collecting and maintaining the Private Information, the Washington Post agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs Bryant, Bennett, Nance, Hatzipanagos, and Leiby and relevant Class Members themselves took reasonable steps to secure their Private Information. Under state and federal law, the Washington Post has duties to protect the Private Information of its current and former employees and contractors and to notify them about data breaches.

214. The Washington Post recognizes these duties, advertising in its "Privacy Policy" that:

a. "This Privacy Policy (or 'Policy') explains how WP Company LLC ('The Washington Post,' 'we,' or 'us') collects, uses, and discloses information about you[.]"[180]

b. "Data Security. We have in place physical, electronic and managerial procedures to help protect the information we collect."[181]

215. On information and belief, the Washington Post selected Oracle as a third-party vendor and then input the Private Information of its current and former employees and contractors

[180] *Privacy Policy* THE WASHINGTON POST, https://www.washingtonpost.com/privacy-policy/ (last visited Feb. 26, 2026).
[181] *Id*.

into the Oracle EBS system. In doing so, the Washington Post disclosed the Private Information of its current and former employees and contractors to Oracle.

216. Thus far, the Washington Post has admitted that:

a. "On September 29, 2025, the Post was contacted by a bad actor who claimed to have gained access to its Oracle E-Business Suite applications."[182]

b. "In response, the Post launched a thorough investigation of its Oracle application environment with the assistance of experts to determine if the environment had been accessed without authorization."[183]

c. "During the investigation, Oracle announced that it had identified a previously unknown and widespread vulnerability in its E-Business Suite software that permitted unauthorized actors to access many Oracle customers' E-Business Suite applications."[184]

d. "The Post's investigation confirmed that it was impacted by this exploit and determined that, between July 10, 2025, and August 22, 2025, certain data was accessed and acquired without authorization."[185]

e. "On October 27, 2025, the Post confirmed that certain personal information belonging to current and former employees and contractors was affected by this incident."[186]

---

[182] *Data Breach Notifications*, MAINE ATTY GEN (Nov. 12, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/12a31419-4ed0-41ba-a045-2593908ba368.html.
[183] *Id*.
[184] *Id*.
[185] *Id*.
[186] *Id*.

f. "The affected information varies by individual but may include individuals' names, bank account numbers and associated routing numbers, Social Security numbers, and/or tax ID numbers."[187]

217. Thus far, the Washington Post has stated that 9,720 of its current and former employees and contractors were exposed.[188]

218. But on or around January 2026, CL0P published on its Dark Web leak site approximately 183.55 gibibytes of data including approximately 29,000 different Social Security numbers that appear to originate from the Washington Post.

219. Based on these facts, CL0P has already published the Private Information that CL0P obtained from the Washington Post during the Data Breach.

220. And yet, the Washington Post waited until November 12, 2025, before providing a notification about the Data Breach.[189] The Washington Post kept Plaintiffs Bryant, Bennett, Nance, Hatzipanagos, and Leiby and relevant Class Members in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

221. Notably, the Washington Post acknowledged that the Data Breach created a present, continuing, and significant risk of identity theft—warning recipients of the notice that "we recommend that you remain vigilant by reviewing your account statements and credit reports closely."[190]

222. The Washington Post breached its duties by failing to audit and monitor the software of its third-party vendor for vulnerabilities, failing to timely implement software patches,

[187] *Id.*
[188] *Id*
[189] *Id.*
[190] *Id.*

failing to ensure that the Private Information that it provided to Oracle was encrypted at rest and in transit, failing to redact or delete data from Oracle that it was not required to maintain, and/or by failing to monitor its Oracle instance for unusual activity and the transfer of large volumes of data to third party networks.

223. Through its breaches, the Washington Post injured Plaintiffs Kim, Bryant, Bennett, Nance, Hatzipanagos, and Leiby and relevant Class Members.

V. EXPERIENCES AND INJURIES OF PLAINTIFFS

Plaintiff Matthew Tannehill

224. Plaintiff Matthew Tannehill is a former employee of Anywhere.

225. Anywhere required that Plaintiff Tannehill disclose his Private Information. Thus, Anywhere obtained and maintained his Private Information.

226. On information and belief, the types of Private Information that Anywhere obtained and maintained from Plaintiff Tannehill included his name, address, Social Security number, financial account information (including his bank account information and 401k information), and health records.

227. On information and belief, Anywhere disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

228. As a result, Plaintiff Tannehill was injured by the Data Breach.

229. Plaintiff Tannehill is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

230. Plaintiff Tannehill (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

231. Plaintiff Tannehill reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

232. Plaintiff Tannehill does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

233. Through their Data Breach, Defendants compromised Plaintiff's Private Information.

234. As described herein, the Private Information of Plaintiff Tannehill has already been published—or will be published imminently—by CL0P on the Dark Web.

235. In response to the risks created by the Data Breach, Plaintiff Tannehill has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Tannehill has lost approximately three (3) hours researching the Data Breach, investigating fraud, and monitoring his accounts for suspicious activity.

236. Because of the Data Breach, Plaintiff Tannehill anticipates spending considerable amounts of time and money to try and mitigate his injuries.

237. In the aftermath of the Data Breach, Plaintiff Tannehill suffered from a spike in suspicious spam and scam text messages and/or phone calls.

238. Plaintiff Tannehill fears for his personal financial security and worries about what information was exposed in the Data Breach.

239. Because of the Data Breach, Plaintiff Tannehill has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

240. Plaintiff Tannehill suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

241. Plaintiff Tannehill suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

242. As a former employee, Plaintiff Tannehill suffered actual injury and lost the "benefit of the bargain" when Plaintiff Tannehill (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about their deficient data security, then Plaintiff Tannehill would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

243. Plaintiff Tannehill suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

244. Today, Plaintiff Tannehill has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Michael Nero

245. Plaintiff Michael Nero is a former employee of Cartus Corporation which is a subsidiary of Anywhere.

246. Anywhere required that Plaintiff Nero disclose his Private Information. Thus, Anywhere obtained and maintained his Private Information.

247. On information and belief, the types of Private Information that Anywhere obtained and maintained from Plaintiff Nero included his name, address, contact information, date of birth, and Social Security number.

248. On information and belief, Anywhere disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

249. As a result, Plaintiff Nero was injured by the Data Breach.

250. Plaintiff Nero is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

251. Plaintiff Nero (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

252. Plaintiff Nero reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

253. Plaintiff Nero received a Notice of Data Breach from Anywhere.

254. Through their Data Breach, Defendants compromised Plaintiff's Private Information.

255. As described herein, the Private Information of Plaintiff Nero has already been published—or will be published imminently—by CL0P on the Dark Web.

256. In response to the risks created by the Data Breach, Plaintiff Nero has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Nero has lost approximately three (3) hours researching the data breach and monitoring his accounts for suspicious activity.

257. Because of the Data Breach, Plaintiff Nero anticipates spending considerable amounts of time and money to try and mitigate his injuries.

258. In the aftermath of the Data Breach, Plaintiff Nero suffered from a spike in suspicious spam and scam text messages and/or phone calls.

259. Plaintiff Nero fears for his personal financial security and worries about what information was exposed in the Data Breach.

260. Because of the Data Breach, Plaintiff Nero has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

261. Plaintiff Nero suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

262. Plaintiff Nero suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

263. As a former employee, Plaintiff Nero suffered actual injury and lost the "benefit of the bargain" when Plaintiff Nero (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Nero would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

264. Plaintiff Nero suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

265. Today, Plaintiff Nero has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff James Massengill

266. Plaintiff James Massengill is a former employee of Cox.

267. Cox required that Plaintiff Massengill disclose his Private Information. Thus, Cox obtained and maintained his Private Information.

268. On information and belief, the types of Private Information that Cox obtained and maintained from Plaintiff Massengill included his name, address, Social Security number, date of birth, phone number, email address, and financial account information (bank account numbers and payment information).

269. On information and belief, Cox disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

270. As a result, Plaintiff Massengill was injured by the Data Breach.

271. Plaintiff Massengill is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

272. Plaintiff Massengill (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

273. Plaintiff Massengill reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

274. Plaintiff Massengill received a Notice of Data Breach from Cox dated November 20, 2025.

275. Through their Data Breach, Defendants compromised Plaintiff Massengill's Private Information.

276. As described herein, the Private Information of Plaintiff Massengill has already been published—or will be published imminently—by CL0P on the Dark Web.

277. In response to the risks created by the Data Breach, Plaintiff Massengill has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Massengill has lost approximately twenty (20) hours researching the data breach, contacting credit bureaus, contacting his financial institution, and monitoring his accounts for suspicious activity.

278. Because of the Data Breach, Plaintiff Massengill anticipates spending considerable amounts of time and money to try and mitigate his injuries.

279. In the aftermath of the Data Breach, Plaintiff Massengill suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

280. Plaintiff Massengill fears for his personal financial security and worries about what information was exposed in the Data Breach.

281. Because of the Data Breach, Plaintiff Massengill has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

282. Plaintiff Massengill suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

283. Plaintiff Massengill suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

284. As a former employee, Plaintiff Massengill suffered actual injury and lost the "benefit of the bargain" when Plaintiff Massengill (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Massengill would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

285. Plaintiff Massengill suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Massengill's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

286. Today, Plaintiff Massengill has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Marcus Issac

287. Plaintiff Marcus Issac is a former employee of Cox.

288. Cox required that Plaintiff Issac disclose his Private Information. Thus, Cox obtained and maintained his Private Information.

289. On information and belief, the types of Private Information that Cox obtained and maintained from Plaintiff Issac included his name, Social Security number, date of birth, contact information, financial account information, and insurance information.

290. On information and belief, Cox disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

291. As a result, Plaintiff Issac was injured by the Data Breach.

292. Plaintiff Issac is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

293. Plaintiff Issac (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

294. Plaintiff Issac reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

295. Plaintiff Issac does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

296. Through their Data Breach, Defendants compromised Plaintiff Issac's Private Information.

297. As described herein, the Private Information of Plaintiff Issac has already been published—or will be published imminently—by CL0P on the Dark Web.

298. In response to the risks created by the Data Breach, Plaintiff Issac has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Issac has lost approximately two (2) hours per day researching the Data Breach and monitoring his accounts for suspicious activity.

299. Because of the Data Breach, Plaintiff Issac anticipates spending considerable amounts of time and money to try and mitigate his injuries.

300. In the aftermath of the Data Breach, Plaintiff Issac suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

301. Plaintiff Issac fears for his personal financial security and worries about what information was exposed in the Data Breach.

302. Because of the Data Breach, Plaintiff Issac has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

303. Plaintiff Issac suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

304. Plaintiff Issac suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

305. As a former employee, Plaintiff Issac suffered actual injury and lost the "benefit of the bargain" when Plaintiff Issac (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Issac would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

306. Plaintiff Issac suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach

placed Plaintiff Issac's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

307. Today, Plaintiff Issac has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Leonid Koyfman

308. Plaintiff Leonid Koyfman is a former employee of GlobalLogic.

309. GlobalLogic required that Plaintiff Koyfman disclose his Private Information. Thus, GlobalLogic obtained and maintained his Private Information.

310. On information and belief, the types of Private Information that GlobalLogic obtained and maintained from Plaintiff Koyfman included his "name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, internal GlobalLogic employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."

311. On information and belief, GlobalLogic disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

312. As a result, Plaintiff Koyfman was injured by the Data Breach.

313. Plaintiff Koyfman is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

314. Plaintiff Koyfman (or his third-party agent) provided his Private Information to Oracle and trusted it would use reasonable measures to protect it according to its internal policies, as well as state and federal law. Oracle obtained and continues to maintain his Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

315. Plaintiff Koyfman reasonably understood that a portion of the funds paid to Oracle (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

316. Plaintiff Koyfman does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

317. Plaintiff Koyfman received a Notice of Data Breach from GlobalLogic dated November 10, 2025.

318. Through their Data Breach, Oracle compromised Plaintiff Koyfman's Private Information.

319. As described herein, the Private Information of Plaintiff Koyfman has already been published—or will be published imminently—by CL0P on the Dark Web.

320. In response to the risks created by the Data Breach, Plaintiff Koyfman has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Koyfman has lost approximately eight (8) hours responding to the Data Breach.

321. Because of the Data Breach, Plaintiff Koyfman anticipates spending considerable amounts of time and money to try and mitigate his injuries.

322. In the aftermath of the Data Breach, Plaintiff Koyfman suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

323. Plaintiff Koyfman fears for his personal financial security and worries about what information was exposed in the Data Breach.

324. Because of the Data Breach, Plaintiff Koyfman has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

325. Plaintiff Koyfman suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

326. Plaintiff Koyfman suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Oracle was required to adequately protect.

327. Plaintiff Koyfman suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Koyfman's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

328. Today, Plaintiff Koyfman has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Oracle—is protected and safeguarded from additional breaches.

Plaintiff Micheil Boggs

329. Micheil Boggs, through the intermediary Braven Inc., is a former employee or contractor of GlobalLogic.

330. GlobalLogic required that Plaintiff Boggs disclose his Private Information. Thus, GlobalLogic obtained and maintained his Private Information.

331. On information and belief, the types of Private Information that GlobalLogic obtained and maintained from Plaintiff Boggs included his "name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, internal GlobalLogic employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."

332. On information and belief, GlobalLogic disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

333. As a result, Plaintiff Boggs was injured by the Data Breach.

334. Plaintiff Boggs is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

335. Plaintiff Boggs (or his third-party agent) provided his Private Information to Oracle and trusted it would use reasonable measures to protect it according to its internal policies, as well as state and federal law. Oracle obtained and continues to maintain his Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

336. Plaintiff Boggs reasonably understood that a portion of the funds paid to Oracle (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

337. Plaintiff Boggs received a Notice of Data Breach from GlobalLogic dated November 10, 2025.

338. Through their Data Breach, Oracle compromised Plaintiff Boggs's Private Information.

339. After the Data Breach, Plaintiff Boggs suffered from the misuse of his Private Information when cybercriminals from foreign countries attempted to log into his Microsoft, Facebook, and email accounts.

340. As described herein, the Private Information of Plaintiff Boggs has already been published—or will be published imminently—by CL0P on the Dark Web.

341. In response to the risks created by the Data Breach, Plaintiff Boggs has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Boggs has lost approximately two (2) hours per week researching the Data Breach, updating his passwords, and monitoring his accounts for suspicious activity.

342. Because of the Data Breach, Plaintiff Boggs anticipates spending considerable amounts of time and money to try and mitigate his injuries.

343. Starting in August 2025, Plaintiff Boggs suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

344. Plaintiff Boggs fears for his personal financial security and worries about what information was exposed in the Data Breach.

345. Because of the Data Breach, Plaintiff Boggs has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

346. Plaintiff Boggs suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

347. Plaintiff Boggs suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Oracle was required to adequately protect.

348. Plaintiff Boggs suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Boggs's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

349. Today, Plaintiff Boggs has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Oracle—is protected and safeguarded from additional breaches.

Plaintiff Patricia Eagan

350. Patricia Eagan is a former employee or contractor of GlobalLogic.

351. GlobalLogic required that Plaintiff Eagan disclose her Private Information. Thus, GlobalLogic obtained and maintained her Private Information.

352. On information and belief, the types of Private Information that GlobalLogic obtained and maintained from Plaintiff Eagan included her "name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."

353. On information and belief, GlobalLogic disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

354. As a result, Plaintiff Eagan was injured by the Data Breach.

355. Plaintiff Eagan is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

356. Plaintiff Eagan (or her third-party agent) provided her Private Information to Oracle and trusted it would use reasonable measures to protect it according to its internal policies, as well as state and federal law. Oracle obtained and continues to maintain her Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

357. Plaintiff Eagan reasonably understood that a portion of the funds paid to Oracle (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

358. Plaintiff Eagan received a Notice of Data Breach by email from GlobalLogic.

359. Through their Data Breach, Oracle compromised Plaintiff Eagan's Private Information.

360. As described herein, the Private Information of Plaintiff Eagan has already been published—or will be published imminently—by CL0P on the Dark Web.

361. In response to the risks created by the Data Breach, Plaintiff Eagan has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Eagan has lost approximately three (3) hours per week

researching the Data Breach, freezing her credit, and monitoring her accounts for suspicious activity.

362. After the Data Breach, and in response to the risks created by the Data Breach, Plaintiff Eagan ***paid out-of-pocket*** for a monthly subscription to the identity protection service "Aura" at $13.99 per month to try and protect herself from the risks created by the Data Breach.

363. Because of the Data Breach, Plaintiff Eagan anticipates spending considerable amounts of time and money to try and mitigate her injuries.

364. In the aftermath of the Data Breach, Plaintiff Eagan suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

365. Plaintiff Eagan fears for her personal financial security and worries about what information was exposed in the Data Breach.

366. Because of the Data Breach, Plaintiff Eagan has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

367. Plaintiff Eagan suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

368. Plaintiff Eagan suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Oracle was required to adequately protect.

369. Plaintiff Eagan suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach

placed Plaintiff Eagan's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

370. Today, Plaintiff Eagan has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Oracle—is protected and safeguarded from additional breaches.

Plaintiff Ashley Sainvil

371. Ashley Sainvil is a current employee of GlobalLogic.

372. GlobalLogic required that Plaintiff Sainvil disclose her Private Information. Thus, GlobalLogic obtained and maintained her Private Information.

373. On information and belief, the types of Private Information that GlobalLogic obtained and maintained from Plaintiff Sainvil included her "name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."

374. On information and belief, GlobalLogic disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

375. As a result, Plaintiff Sainvil was injured by the Data Breach.

376. Plaintiff Sainvil is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

377. Plaintiff Sainvil (or her third-party agent) provided her Private Information to Oracle and trusted it would use reasonable measures to protect it according to its internal policies,

as well as state and federal law. Oracle obtained and continues to maintain her Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

378. Plaintiff Sainvil reasonably understood that a portion of the funds paid to Oracle (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

379. Plaintiff Sainvil does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

380. Plaintiff Sainvil received a Notice of Data Breach from GlobalLogic on November 13, 2025.

381. Through their Data Breach, Oracle compromised Plaintiff Sainvil's Private Information.

382. As described herein, the Private Information of Plaintiff Sainvil has already been published—or will be published imminently—by CL0P on the Dark Web.

383. In response to the risks created by the Data Breach, Plaintiff Sainvil has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Sainvil has lost approximately thirty (30) hours researching the data breach and monitoring her accounts for suspicious activity.

384. Because of the Data Breach, Plaintiff Sainvil anticipates spending considerable amounts of time and money to try and mitigate her injuries.

385. In the aftermath of the Data Breach, Plaintiff Sainvil suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

386. Plaintiff Sainvil fears for her personal financial security and worries about what information was exposed in the Data Breach.

387. Because of the Data Breach, Plaintiff Sainvil has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

388. Plaintiff Sainvil suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

389. Plaintiff Sainvil suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Oracle was required to adequately protect.

390. Plaintiff Sainvil suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Sainvil's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

391. Today, Plaintiff Sainvil has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Oracle—is protected and safeguarded from additional breaches.

Plaintiff Lisa Magnusson

392. Lisa Magnusson is a former employee of GlobalLogic.

393. GlobalLogic required that Plaintiff Magnusson disclose her Private Information. Thus, GlobalLogic obtained and maintained her Private Information.

394. On information and belief, the types of Private Information that GlobalLogic obtained and maintained from Plaintiff Magnusson included her name, "name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."

395. On information and belief, GlobalLogic disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

396. As a result, Plaintiff Magnusson was injured by the Data Breach.

397. Plaintiff Magnusson is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

398. Plaintiff Magnusson (or her third-party agent) provided her Private Information to Oracle and trusted it would use reasonable measures to protect it according to its internal policies, as well as state and federal law. Oracle obtained and continues to maintain her Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

399. Plaintiff Magnusson reasonably understood that a portion of the funds paid to Oracle (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

400. Through their Data Breach, Oracle compromised Plaintiff Magnusson's Private Information.

401. Plaintiff Magnusson has ***already suffered*** from identity theft and fraud—whereby cybercriminals placed a fraudulent charge on her bank account for approximately $500 in or around September 2025.

402. As described herein, the Private Information of Plaintiff Magnusson has already been published—or will be published imminently—by CL0P on the Dark Web.

403. In response to the risks created by the Data Breach, Plaintiff Magnusson has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Magnusson has lost approximately ten (10) hours monitoring her accounts for suspicious activity, investigating fraud, and contacting her bank.

404. Because of the Data Breach, Plaintiff Magnusson anticipates spending considerable amounts of time and money to try and mitigate her injuries.

405. In the aftermath of the Data Breach, Plaintiff Magnusson suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

406. Plaintiff Magnusson fears for her personal financial security and worries about what information was exposed in the Data Breach.

407. Because of the Data Breach, Plaintiff Magnusson has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

408. Plaintiff Magnusson suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

409. Plaintiff Magnusson suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Oracle was required to adequately protect.

410. Plaintiff Magnusson suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Magnusson's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

411. Today, Plaintiff Magnusson has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Oracle—is protected and safeguarded from additional breaches.

Plaintiff Arianna Brown

412. Plaintiff Arianna Brown is a former employee of GlobalLogic.

413. GlobalLogic required that Plaintiff Brown disclose her Private Information. Thus, GlobalLogic obtained and maintained her Private Information.

414. On information and belief, the types of Private Information that GlobalLogic obtained and maintained from Plaintiff Brown included her name, "name, address, phone number, emergency contact (name and phone number), email, date of birth, nationality, country of birth, passport information, employee number, national identifier or tax identifier such as Social Security Number, salary information, bank account information, and routing number."

415. On information and belief, GlobalLogic disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

416. As a result, Plaintiff Brown was injured by the Data Breach.

417. Plaintiff Brown is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

418. Plaintiff Brown (or her third-party agent) provided her Private Information to Oracle and trusted it would use reasonable measures to protect it according to its internal policies, as well as state and federal law. Oracle obtained and continues to maintain her Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

419. Plaintiff Brown reasonably understood that a portion of the funds paid to Oracle (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

420. Through their Data Breach, Oracle compromised Plaintiff Brown's Private Information.

421. Plaintiff Brown has ***already suffered*** from identity theft and fraud—whereby cybercriminals stole her identity and placed a fraudulent charge on her Navy Federal Credit Union debit card for $544.86 at "TARGET.COM" on October 9, 2025.

422. Notably, Plaintiff had previously disclosed her financial account information for Navy Federal Credit Union to GlobalLogic for the purposes of direct deposit. And GlobalLogic used her account with Navy Federal Credit and deposited her paycheck into that account.

423. As described herein, the Private Information of Plaintiff Brown has already been published—or will be published imminently—by CL0P on the Dark Web.

424. In response to the risks created by the Data Breach, Plaintiff Brown has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Brown has lost approximately two (2) hours researching the Data Breach, monitoring her accounts for suspicious activity, investigating fraud, and contacting her bank.

425. Because of the Data Breach, Plaintiff Brown anticipates spending considerable amounts of time and money to try and mitigate her injuries.

426. In the aftermath of the Data Breach, Plaintiff Brown suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

427. Plaintiff Brown fears for her personal financial security and worries about what information was exposed in the Data Breach.

428. Because of the Data Breach, Plaintiff Brown has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

429. Plaintiff Brown suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

430. Plaintiff Brown suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Oracle was required to adequately protect.

431. Plaintiff Brown suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach

placed Plaintiff Brown's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

432. Today, Plaintiff Brown has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Oracle—is protected and safeguarded from additional breaches.

Plaintiff KaSandra Reynolds

433. Plaintiff KaSandra Reynolds is a former employee of LKQ.

434. LKQ required that Plaintiff Reynolds disclose her Private Information. Thus, LKQ obtained and maintained her Private Information.

435. On information and belief, the types of Private Information that LKQ obtained and maintained from Plaintiff Reynolds included her name, Social Security number, date of birth, contact information, financial account information, and insurance information.

436. On information and belief, LKQ disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

437. As a result, Plaintiff Reynolds was injured by the Data Breach.

438. Plaintiff Reynolds is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

439. Plaintiff Reynolds (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private

Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

440. Plaintiff Reynolds reasonably understood that a portion of the funds paid to Defendants (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

441. Plaintiff Reynolds does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

442. Through their Data Breach, Defendants compromised Plaintiff Reynolds's Private Information.

443. Plaintiff Reynolds has ***already suffered*** from identity theft and fraud:

a. In or around October 2025, cybercriminals stole her identity and placed a fraudulent charge at a gas station using her Visa card with US Bank.

b. On or around January 26, 2026, she was notified by her bank USAA that an identity thief was attempting to transfer approximately $1,000 out of her account into an unfamiliar account in Chicago, Illinois.

444. As described herein, the Private Information of Plaintiff Reynolds has already been published—or will be published imminently—by CL0P on the Dark Web.

445. In response to the risks created by the Data Breach, Plaintiff Reynolds has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Reynolds has lost approximately twenty-four (24) hours researching the Data Breach, contacting her banks, investigating fraud, and monitoring her accounts for suspicious activity.

446. Because of the Data Breach, Plaintiff Reynolds anticipates spending considerable amounts of time and money to try and mitigate her injuries.

447. Plaintiff Reynolds fears for her personal financial security and worries about what information was exposed in the Data Breach.

448. Because of the Data Breach, Plaintiff Reynolds has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

449. Plaintiff Reynolds suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

450. Plaintiff Reynolds suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

451. As a former employee, Plaintiff Reynolds suffered actual injury and lost the "benefit of the bargain" when Plaintiff Reynolds (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Reynolds would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

452. Plaintiff Reynolds suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Reynolds's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

453. Today, Plaintiff Reynolds has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Christian Alvarado

454. Plaintiff Christian Alvarado is a former employee of MSG.

455. MSG required that Plaintiff Alvarado disclose his Private Information. Thus, MSG obtained and maintained his Private Information.

456. On information and belief, the types of Private Information that MSG obtained and maintained from Plaintiff Alvarado included his name, date of birth, Social Security number, financial account information, tax information, and contact information.

457. On information and belief, MSG disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

458. As a result, Plaintiff Alvarado was injured by the Data Breach.

459. Plaintiff Alvarado is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

460. Plaintiff Alvarado (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

461. Plaintiff Alvarado reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

462. Through their Data Breach, Defendants compromised Plaintiff Alvarado's Private Information.

463. As described herein, the Private Information of Plaintiff Alvarado has already been published—or will be published imminently—by CL0P on the Dark Web.

464. In response to the risks created by the Data Breach, Plaintiff Alvarado has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Alvarado has lost approximately one (1) hour researching the Data Breach.

465. Because of the Data Breach, Plaintiff Alvarado anticipates spending considerable amounts of time and money to try and mitigate his injuries.

466. In the aftermath of the Data Breach, Plaintiff Alvarado suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

467. Plaintiff Alvarado fears for his personal financial security and worries about what information was exposed in the Data Breach.

468. Because of the Data Breach, Plaintiff Alvarado has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

469. Plaintiff Alvarado suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

470. Plaintiff Alvarado suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

471. As a former employee, Plaintiff Alvarado suffered actual injury and lost the "benefit of the bargain" when Plaintiff Alvarado (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Alvarado would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

472. Plaintiff Alvarado suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Alvarado's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

473. Today, Plaintiff Alvarado has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Angel Liranzo

474. Plaintiff Angel Liranzo is a former employee of MSG.

475. MSG required that Plaintiff Liranzo disclose her Private Information. Thus, MSG obtained and maintained her Private Information.

476. On information and belief, the types of Private Information that MSG obtained and maintained from Plaintiff Liranzo included her Social Security number, driver's license number, date of birth, name, address, email, phone, and other contact information.

477. On information and belief, MSG disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

478. As a result, Plaintiff Liranzo was injured by the Data Breach.

479. Plaintiff Liranzo is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

480. Plaintiff Liranzo (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

481. Plaintiff Liranzo does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

482. Plaintiff Liranzo received a Notice of Data Breach from MSG on or about February 23, 2026.

483. Through their Data Breach, Defendants compromised Plaintiff Liranzo's Private Information.

484. As described herein, the Private Information of Plaintiff Liranzo has already been published—or will be published imminently—by CL0P on the Dark Web.

485. In response to the risks created by the Data Breach, Plaintiff Liranzo has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft.

486. Because of the Data Breach, Plaintiff Liranzo anticipates spending considerable amounts of time and money to try and mitigate her injuries.

487. Plaintiff Liranzo fears for her personal financial security and worries about what information was exposed in the Data Breach.

488. Because of the Data Breach, Plaintiff Liranzo has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

489. Plaintiff Liranzo suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

490. Plaintiff Liranzo suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

491. As a former employee, Plaintiff Liranzo suffered actual injury and lost the "benefit of the bargain" when Plaintiff Liranzo (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Liranzo would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

492. Plaintiff Liranzo suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Liranzo's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

493. Today, Plaintiff Liranzo has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Kevin Youmell

494. Plaintiff Kevin Youmell is a former employee of Parexel.

495. Parexel required that Plaintiff Youmell disclose his Private Information. Thus, Parexel obtained and maintained his Private Information.

496. On information and belief, the types of Private Information that Parexel obtained and maintained from Plaintiff Youmell included his "name, date of birth, financial account number and/or payment card number (without CVV), social security and/or national ID number provided to Parexel in connection with your employment."

497. On information and belief, Parexel disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

498. As a result, Plaintiff Youmell was injured by the Data Breach.

499. Plaintiff Youmell is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

500. Plaintiff Youmell (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

501. Plaintiff Youmell reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

502. Plaintiff Youmell received a Notice of Data Breach from Parexel dated December 17, 2025.

503. Through their Data Breach, Defendants compromised Plaintiff Youmell's Private Information.

504. As described herein, the Private Information of Plaintiff Youmell has already been published—or will be published imminently—by CL0P on the Dark Web.

505. In response to the risks created by the Data Breach, Plaintiff Youmell has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Youmell has lost approximately two (2) hours researching the Data Breach and monitoring his accounts for suspicious activity.

506. Because of the Data Breach, Plaintiff Youmell anticipates spending considerable amounts of time and money to try and mitigate his injuries.

507. In the aftermath of the Data Breach, Plaintiff Youmell suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

508. Plaintiff Youmell fears for his personal financial security and worries about what information was exposed in the Data Breach.

509. Because of the Data Breach, Plaintiff Youmell has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

510. Plaintiff Youmell suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

511. Plaintiff Youmell suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

512. As a former employee, Plaintiff Youmell suffered actual injury and lost the "benefit of the bargain" when Plaintiff Youmell (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Youmell would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

513. Plaintiff Youmell suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Youmell's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

514. Today, Plaintiff Youmell has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Michael Trempus

515. Plaintiff Michael Trempus is a former employee of Parexel.

516. Parexel required that Plaintiff Trempus disclose his Private Information. Thus, Parexel obtained and maintained his Private Information.

517. On information and belief, the types of Private Information that Parexel obtained and maintained from Plaintiff Trempus included his "name, date of birth, financial account number and/or payment card number (without CVV), social security and/or national ID number provided to Parexel in connection with your employment."

518. On information and belief, Parexel disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

519. As a result, Plaintiff Trempus was injured by the Data Breach.

520. Plaintiff Trempus is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

521. Plaintiff Trempus (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

522. Plaintiff Trempus reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

523. Plaintiff Trempus received a Notice of Data Breach from Parexel.

524. Through their Data Breach, Defendants compromised Plaintiff Trempus's Private Information.

525. As described herein, the Private Information of Plaintiff Trempus has already been published—or will be published imminently—by CL0P on the Dark Web.

526. In response to the risks created by the Data Breach, Plaintiff Trempus has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Trempus has lost approximately ten (10) hours researching the Data Breach, contacting credit bureaus, contacting his bank to issue a new credit card, researching credit monitoring options, and monitoring his accounts for suspicious activity.

527. After the Data Breach, and in response to the risks created by the Data Breach, Plaintiff Trempus ***paid out-of-pocket*** for a yearly subscription to the identity protection service "Aura" at $250 per year to try and protect himself from the risks created by the Data Breach.

528. Because of the Data Breach, Plaintiff Trempus anticipates spending considerable amounts of time and money to try and mitigate his injuries.

529. Plaintiff Trempus fears for his personal financial security and worries about what information was exposed in the Data Breach.

530. Because of the Data Breach, Plaintiff Trempus has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

531. Plaintiff Trempus suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

532. Plaintiff Trempus suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

533. As a former employee, Plaintiff Trempus suffered actual injury and lost the "benefit of the bargain" when Plaintiff Trempus (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Trempus would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

534. Plaintiff Trempus suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Trempus's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

535. Today, Plaintiff Trempus has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Nicole O'Keeffe

536. Plaintiff Nicole O'Keeffe is a former employee of Parexel.

537. Parexel required that Plaintiff O'Keeffe disclose her Private Information. Thus, Parexel obtained and maintained her Private Information.

538. On information and belief, the types of Private Information that Parexel obtained and maintained from Plaintiff O'Keeffe included her "name, date of birth, financial account number and/or payment card number (without CVV), social security and/or national ID number provided to Parexel in connection with your employment."

539. On information and belief, Parexel disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

540. As a result, Plaintiff O'Keeffe was injured by the Data Breach.

541. Plaintiff O'Keeffe is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

542. Plaintiff O'Keeffe (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

543. Plaintiff O'Keeffe reasonably understood that a portion of the funds paid to Defendants (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

544. Plaintiff O'Keeffe received a Notice of Data Breach from Parexel dated December 17, 2025.

545. Through their Data Breach, Defendants compromised Plaintiff O'Keeffe's Private Information.

546. Plaintiff O'Keeffe has ***already suffered*** from identity theft and fraud—whereby on December 30, 2025, cybercriminals stole her identity and placed a fraudulent charge of $228.95 for "ANS ENGINEE" on her card with Chase bank.

547. As described herein, the Private Information of Plaintiff O'Keeffe has already been published—or will be published imminently—by CL0P on the Dark Web.

548. In response to the risks created by the Data Breach, Plaintiff O'Keeffe has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff O'Keeffe has lost approximately twelve (12) hours researching the Data Breach, contacting her bank, investigating fraud, and monitoring her accounts for suspicious activity.

549. Because of the Data Breach, Plaintiff O'Keeffe anticipates spending considerable amounts of time and money to try and mitigate her injuries.

550. Plaintiff O'Keeffe fears for her personal financial security and worries about what information was exposed in the Data Breach.

551. Because of the Data Breach, Plaintiff O'Keeffe has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

552. Plaintiff O'Keeffe suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

553. Plaintiff O'Keeffe suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

554. As a former employee, Plaintiff O'Keeffe suffered actual injury and lost the "benefit of the bargain" when Plaintiff O'Keeffe (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff O'Keeffe

would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

555. Plaintiff O'Keeffe suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff O'Keeffe's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

556. Today, Plaintiff O'Keeffe has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Lourdes Naulty

557. Plaintiff Lourdes Naulty is a former employee of Parexel.

558. Parexel required that Plaintiff Naulty disclose her Private Information. Thus, Parexel obtained and maintained her Private Information.

559. On information and belief, the types of Private Information that Parexel obtained and maintained from Plaintiff Naulty included her "name, date of birth, financial account number and/or payment card number (without CVV), social security and/or national ID number provided to Parexel in connection with your employment."

560. On information and belief, Parexel disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

561. As a result, Plaintiff Naulty was injured by the Data Breach.

562. Plaintiff Naulty is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an

unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

563. Plaintiff Naulty (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

564. Plaintiff Naulty reasonably understood that a portion of the funds paid to Defendants (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

565. Through their Data Breach, Defendants compromised Plaintiff Naulty's Private Information.

566. Plaintiff Naulty has ***already suffered*** from identity theft and fraud—whereby on or around November 27, 2025, cybercriminals stole her identity and placed a fraudulent charge of approximately $100 for "Walmart" on her debit card with Chase bank.

567. As described herein, the Private Information of Plaintiff Naulty has already been published—or will be published imminently—by CL0P on the Dark Web.

568. In response to the risks created by the Data Breach, Plaintiff Naulty has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Naulty has lost time responding to the fraudulent charge and canceling her debit card with Chase bank.

569. Because of the Data Breach, Plaintiff Naulty anticipates spending considerable amounts of time and money to try and mitigate her injuries.

570. Plaintiff Naulty fears for her personal financial security and worries about what information was exposed in the Data Breach.

571. Because of the Data Breach, Plaintiff Naulty has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

572. Plaintiff Naulty suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

573. Plaintiff Naulty suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

574. As a former employee, Plaintiff Naulty suffered actual injury and lost the "benefit of the bargain" when Plaintiff Naulty (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Naulty would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

575. Plaintiff Naulty suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Naulty's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

576. Today, Plaintiff Naulty has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Richard Yao

577. Plaintiff Richard Yao is a former graduate student of RF SUNY.

578. RF SUNY required that Plaintiff Yao disclose his Private Information. Thus, RF SUNY obtained and maintained his Private Information.

579. On information and belief, the types of Private Information that RF SUNY obtained and maintained from Plaintiff Yao included his name, contact information, address, date of birth, Social Security number, and financial account information.

580. On information and belief, RF SUNY disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

581. As a result, Plaintiff Yao was injured by the Data Breach.

582. Plaintiff Yao is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

583. Plaintiff Yao (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

584. Plaintiff Yao reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

585. Plaintiff Yao does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

586. Plaintiff Yao received a Notice of Data Breach from RF SUNY dated January 29, 2026.

587. Through their Data Breach, Defendants compromised Plaintiff Yao's Private Information.

588. As described herein, the Private Information of Plaintiff Yao has already been published—or will be published imminently—by CL0P on the Dark Web.

589. In response to the risks created by the Data Breach, Plaintiff Yao has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Yao has lost approximately forty-five (45) minutes researching the Data Breach and monitoring his account for suspicious activity.

590. Because of the Data Breach, Plaintiff Yao anticipates spending considerable amounts of time and money to try and mitigate his injuries.

591. In the aftermath of the Data Breach, Plaintiff Yao suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

592. Plaintiff Yao fears for his personal financial security and worries about what information was exposed in the Data Breach.

593. Because of the Data Breach, Plaintiff Yao has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

594. Plaintiff Yao suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

595. Plaintiff Yao suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

596. As a former student, Plaintiff Yao suffered actual injury and lost the "benefit of the bargain" because Plaintiff Yao paid Defendants for services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all, if Defendants were transparent about its deficient data security, then Plaintiff Yao (1) would have either declined to become a customer of Defendants and would have taken his business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

597. As a former employee, Plaintiff Yao suffered actual injury and lost the "benefit of the bargain" when Plaintiff Yao (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Yao would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

598. Plaintiff Yao suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Yao's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

599. Today, Plaintiff Yao has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Matthew Ross

600. Plaintiff Matthew Ross is a former student of Dartmouth.

601. Dartmouth required that Plaintiff Ross disclose his Private Information. Thus, Dartmouth obtained and maintained his Private Information.

602. On information and belief, the types of Private Information that Dartmouth obtained and maintained from Plaintiff Ross included his name, address, date of birth, Social Security number, and financial account information.

603. On information and belief, Dartmouth disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

604. As a result, Plaintiff Ross was injured by the Data Breach.

605. Plaintiff Ross is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

606. Plaintiff Ross (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

607. Plaintiff Ross reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of Private Information.

608. Plaintiff Ross received a Notice of Data Breach from Dartmouth on November 24, 2025—stating that "We are writing to inform you of a data security incident that involved your information including your name, Social Security number, and financial account information."

609. Through their Data Breach, Defendants compromised Plaintiff Ross's Private Information.

610. As described herein, the Private Information of Plaintiff Ross has already been published—or will be published imminently—by CL0P on the Dark Web.

611. In response to the risks created by the Data Breach, Plaintiff Ross has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Ross has lost approximately twenty (20) hours researching the Data Breach, researching how to reduce the influx in scam calls, and monitoring his credit.

612. Because of the Data Breach, Plaintiff Ross anticipates spending considerable amounts of time and money to try and mitigate his injuries.

613. In the aftermath of the Data Breach, Plaintiff Ross suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

614. Plaintiff Ross fears for his personal financial security and worries about what information was exposed in the Data Breach.

615. Because of the Data Breach, Plaintiff Ross has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

616. Plaintiff Ross suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

617. Plaintiff Ross suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

618. As a former student, Plaintiff Ross suffered actual injury and lost the "benefit of the bargain" because Plaintiff Ross paid Defendants for products/services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all, if Defendants were transparent about its deficient data security, then Plaintiff Ross (1) would have either declined to become a customer of Defendants and would have taken his business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

619. Plaintiff Ross suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Ross's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

620. Today, Plaintiff Ross has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Lisa Mabey

621. Plaintiff Lisa Mabey is a former patient of the Dartmouth Hitchcock Medical Center.

622. Dartmouth required that Plaintiff Mabey disclose her Private Information. Thus, Dartmouth obtained and maintained her Private Information.

623. On information and belief, the types of Private Information that Dartmouth obtained and maintained from Plaintiff Mabey included her name, Social Security number, financial account information, and protected health information.

624. On information and belief, Dartmouth disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

625. As a result, Plaintiff Mabey was injured by the Data Breach.

626. Plaintiff Mabey is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

627. Plaintiff Mabey (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

628. Plaintiff Mabey reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of Private Information.

629. Plaintiff Mabey does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

630. Plaintiff Mabey received a Notice of Data Breach from Dartmouth dated November 24, 2025. Therein, Dartmouth confirmed that at least her "name, Social Security number, and financial account information" were compromised.

631. Through their Data Breach, Defendants compromised Plaintiff Mabey's Private Information.

632. As described herein, the Private Information of Plaintiff Mabey has already been published—or will be published imminently—by CL0P on the Dark Web.

633. In response to the risks created by the Data Breach, Plaintiff Mabey has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Mabey has lost approximately three (3) hours researching the Data Breach and seeking legal representation.

634. Because of the Data Breach, Plaintiff Mabey anticipates spending considerable amounts of time and money to try and mitigate her injuries.

635. Plaintiff Mabey fears for her personal financial security and worries about what information was exposed in the Data Breach.

636. Because of the Data Breach, Plaintiff Mabey has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

637. Plaintiff Mabey suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

638. Plaintiff Mabey suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

639. As a former patient, Plaintiff Mabey suffered actual injury and lost the "benefit of the bargain" because Plaintiff Mabey paid Defendants for services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all, if Defendants were transparent about its deficient data security, then Plaintiff Mabey (1) would have either declined to become a customer of Defendants and would have taken her business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

640. Plaintiff Mabey suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Mabey's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

641. Today, Plaintiff Mabey has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Maxim Gilula

642. Plaintiff Maxim Gilula is a former graduate student of UPenn.

643. UPenn required that Plaintiff Gilula disclose his Private Information. Thus, UPenn obtained and maintained his Private Information.

644. On information and belief, the types of Private Information that UPenn obtained and maintained from Plaintiff Gilula included his name, date of birth, Social Security number,

address, contact information, phone number, email address, financial account information (including his bank account number and routing number for direct deposit), and health insurance information.

645. On information and belief, UPenn disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

646. As a result, Plaintiff Gilula was injured by the Data Breach.

647. Plaintiff Gilula is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

648. Plaintiff Gilula (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

649. Plaintiff Gilula reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

650. Plaintiff Gilula does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

651. Plaintiff Gilula received a Notice of Data Breach from UPenn.

652. Through their Data Breach, Defendants compromised Plaintiff Gilula's Private Information.

653. Plaintiff Gilula has ***already suffered*** from identity theft and fraud—and in or around November 2025, Plaintiff discovered that cybercriminals had used his name and Social Security number to apply for, and successfully obtain, approximately $20,000 in fraudulent student loans at the University of Texas Permian Basin. Plaintiff discovered that his identity was stolen in or around November 2025 because his credit score dropped significantly due to the fraudulent loan.

654. Notably, to obtain the fraudulent loans, the identity thieves used the same address that Plaintiff Gilula had provided to UPenn.

655. As described herein, the Private Information of Plaintiff Gilula has already been published—or will be published imminently—by CL0P on the Dark Web.

656. In response to the risks created by the Data Breach, Plaintiff Gilula has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Gilula has lost approximately thirty (30) hours researching the Data Breach and communicating with the IRS to try and address the fraudulent loans.

657. Because of the Data Breach, Plaintiff Gilula anticipates spending considerable amounts of time and money to try and mitigate his injuries.

658. In the aftermath of the Data Breach, Plaintiff Gilula suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

659. Plaintiff Gilula fears for his personal financial security and worries about what information was exposed in the Data Breach.

660. Because of the Data Breach, Plaintiff Gilula has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

661. Plaintiff Gilula suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

662. Plaintiff Gilula suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

663. As a former student, Plaintiff Gilula suffered actual injury and lost the "benefit of the bargain" because Plaintiff Gilula paid Defendants for services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all, if Defendants were transparent about its deficient data security, then Plaintiff Gilula (1) would have either declined to become a customer of Defendants and would have taken his business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

664. In the alternative, as a former employee, Plaintiff Gilula suffered actual injury and lost the "benefit of the bargain" when Plaintiff Gilula (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Gilula would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

665. Plaintiff Gilula suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach

placed Plaintiff Gilula's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

666. Today, Plaintiff Gilula has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Thomas Mosby

667. Plaintiff Thomas Mosby is a current employee of the University of Phoenix.

668. The University of Phoenix required that Plaintiff Mosby disclose his Private Information. Thus, the University of Phoenix obtained and maintained his Private Information.

669. On information and belief, the types of Private Information that the University of Phoenix obtained and maintained from Plaintiff Mosby included his name, Social Security number, phone number, driver's license number, health insurance information, and financial account information.

670. On information and belief, the University of Phoenix disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

671. As a result, Plaintiff Mosby was injured by the Data Breach.

672. Plaintiff Mosby is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

673. Plaintiff Mosby (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private

Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

674. Plaintiff Mosby reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

675. Plaintiff Mosby received a Notice of Data Breach from the University of Phoenix dated December 22, 2025.

676. Through their Data Breach, Defendants compromised Plaintiff Mosby's Private Information.

677. As described herein, the Private Information of Plaintiff Mosby has already been published—or will be published imminently—by CL0P on the Dark Web.

678. Because of the Data Breach, Plaintiff Mosby anticipates spending considerable amounts of time and money to try and mitigate his injuries.

679. In the aftermath of the Data Breach, Plaintiff Mosby suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

680. Plaintiff Mosby fears for his personal financial security and worries about what information was exposed in the Data Breach.

681. Because of the Data Breach, Plaintiff Mosby has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

682. Plaintiff Mosby suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

683. Plaintiff Mosby suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

684. As a former employee, Plaintiff Mosby suffered actual injury and lost the "benefit of the bargain" when Plaintiff Mosby (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Mosby would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

685. Plaintiff Mosby suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Mosby's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

686. Today, Plaintiff Mosby has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Stacy Ranson

687. Plaintiff Stacy Ranson is a former employee and student of the University of Phoenix.

688. The University of Phoenix required that Plaintiff Ranson disclose her Private Information. Thus, the University of Phoenix obtained and maintained her Private Information.

689. On information and belief, the types of Private Information that the University of Phoenix obtained and maintained from Plaintiff Ranson included her name, date of birth, Social Security number, contact information, payroll information, and financial account information.

690. On information and belief, the University of Phoenix disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

691. As a result, Plaintiff Ranson was injured by the Data Breach.

692. Plaintiff Ranson is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

693. Plaintiff Ranson (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

694. Through their Data Breach, Defendants compromised Plaintiff Ranson's Private Information.

695. Plaintiff Ranson has ***already suffered*** from identity theft and fraud—whereby in or around October 2025, cybercriminals placed a series of fraudulent charges on her debit card. Thereafter, Plaintiff spent time disputing the fraudulent charges. Her bank refunded some but not all of the fraudulent charges. Thus, Plaintiff incurred out-of-pocket monetary losses.

696. As described herein, the Private Information of Plaintiff Ranson has already been published—or will be published imminently—by CL0P on the Dark Web.

697. In response to the risks created by the Data Breach, Plaintiff Ranson has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Ranson has lost approximately two (2) hours per week monitoring her accounts for suspicious activity, investigating suspicious activity, and contacting her financial institutions.

698. Because of the Data Breach, Plaintiff Ranson anticipates spending considerable amounts of time and money to try and mitigate her injuries.

699. In the aftermath of the Data Breach, Plaintiff Ranson suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls of up to twenty per day.

700. Plaintiff Ranson fears for her personal financial security and worries about what information was exposed in the Data Breach.

701. Plaintiff Ranson suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

702. Plaintiff Ranson suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

703. As a former student, Plaintiff Ranson suffered actual injury and lost the "benefit of the bargain" because Plaintiff Ranson paid Defendants for services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all, if Defendants were transparent about its deficient data security, then Plaintiff Ranson (1) would have either declined to become a customer of Defendants and would have taken her business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

704. As a former employee, Plaintiff Ranson suffered actual injury and lost the "benefit of the bargain" when Plaintiff Ranson (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Ranson would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

705. Plaintiff Ranson suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Ranson's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

706. Today, Plaintiff Ranson has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Tiaa Pointer

707. Plaintiff Tiaa Pointer is a former student of the University of Phoenix.

708. The University of Phoenix required that Plaintiff Pointer disclose her Private Information. Thus, the University of Phoenix obtained and maintained her Private Information.

709. On information and belief, the types of Private Information that the University of Phoenix obtained and maintained from Plaintiff Pointer included her name, address, phone number, email address, financial account information, and Social Security number.

710. On information and belief, the University of Phoenix disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

711. As a result, Plaintiff Pointer was injured by the Data Breach.

712. Plaintiff Pointer is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

713. Plaintiff Pointer (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

714. Plaintiff Pointer reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of Private Information.

715. Plaintiff Pointer does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

716. Plaintiff Pointer received a Notice of Data Breach from the University of Phoenix dated December 22, 2025.

717. Through their Data Breach, Defendants compromised Plaintiff Pointer's Private Information.

718. Plaintiff Pointer has ***already suffered*** from identity theft and fraud—wherein cybercriminals filed a fraudulent application to Navy Federal Credit Union using her identity.

719. As described herein, the Private Information of Plaintiff Pointer has already been published—or will be published imminently—by CL0P on the Dark Web.

720. In response to the risks created by the Data Breach, Plaintiff Pointer has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself

from identity theft. Specifically, Plaintiff Pointer has lost approximately twenty (20) hours monitoring her accounts for suspicious activity, contacting credit bureaus, contacting the University of Phoenix, and researching the Data Breach and Dark Web exposure.

721. Because of the Data Breach, Plaintiff Pointer anticipates spending considerable amounts of time and money to try and mitigate her injuries.

722. In the aftermath of the Data Breach, Plaintiff Pointer suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

723. Plaintiff Pointer fears for her personal financial security and worries about what information was exposed in the Data Breach.

724. Because of the Data Breach, Plaintiff Pointer has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

725. In fact, the stress caused by the Data Breach exacerbated some of her pre-existing health conditions.

726. Plaintiff Pointer suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

727. Plaintiff Pointer suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

728. As a former student, Plaintiff Pointer suffered actual injury and lost the "benefit of the bargain" because Plaintiff Pointer paid Defendants for services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all,

if Defendants were transparent about its deficient data security, then Plaintiff Pointer (1) would have either declined to become a customer of Defendants and would have taken her business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

729. Plaintiff Pointer suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Pointer's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

730. Today, Plaintiff Pointer has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Luis Vega

731. Plaintiff Luis Vega is a former employee of the University of Phoenix.

732. The University of Phoenix required that Plaintiff Vega disclose his Private Information. Thus, the University of Phoenix obtained and maintained his Private Information.

733. On information and belief, the types of Private Information that the University of Phoenix obtained and maintained from Plaintiff Vega included his name, date of birth, contact information, and Social Security number.

734. On information and belief, the University of Phoenix disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

735. As a result, Plaintiff Vega was injured by the Data Breach.

736. Plaintiff Vega is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe

manner. He is careful to store any documents containing his Private Information in a secure location.

737. Plaintiff Vega (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

738. Plaintiff Vega reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

739. Plaintiff Vega received a Notice of Data Breach from the University of Phoenix.

740. Through their Data Breach, Defendants compromised Plaintiff Vega's Private Information.

741. As described herein, the Private Information of Plaintiff Vega has already been published—or will be published imminently—by CL0P on the Dark Web.

742. In response to the risks created by the Data Breach, Plaintiff Vega has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Vega has lost approximately fifteen (15) hours researching the Data Breach, contacting his financial institutions, and monitoring his accounts for suspicious activity.

743. Because of the Data Breach, Plaintiff Vega anticipates spending considerable amounts of time and money to try and mitigate his injuries.

744. Plaintiff Vega fears for his personal financial security and worries about what information was exposed in the Data Breach.

745. Because of the Data Breach, Plaintiff Vega has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

746. Plaintiff Vega suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

747. Plaintiff Vega suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

748. As a former employee, Plaintiff Vega suffered actual injury and lost the "benefit of the bargain" when Plaintiff Vega (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Vega would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

749. Plaintiff Vega suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Vega's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

750. Today, Plaintiff Vega has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Antonyo Wyche

751. Plaintiff Antonyo Wyche is a former student of the University of Phoenix.

752. The University of Phoenix required that Plaintiff Wyche disclose his Private Information. Thus, the University of Phoenix obtained and maintained his Private Information.

753. On information and belief, the types of Private Information that the University of Phoenix obtained and maintained from Plaintiff Wyche included his name, address, date of birth, financial account information, and Social Security number.

754. On information and belief, the University of Phoenix disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

755. As a result, Plaintiff Wyche was injured by the Data Breach.

756. Plaintiff Wyche is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

757. Plaintiff Wyche (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

758. Plaintiff Wyche reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of Private Information.

759. Plaintiff Wyche received a Notice of Data Breach from the University of Phoenix.

760. Through their Data Breach, Defendants compromised Plaintiff Wyche's Private Information.

761. Plaintiff Wyche has ***already suffered*** from identity theft and fraud—whereby cybercriminals stole his identity and placed fraudulent charges on his checking account with Navy Federal Credit Union including a fraudulent charge of $20.00 on December 8, 2025.

762. Notably, to the best of his recollection, Plaintiff Wyche previously disclosed his financial account information for Navy Federal Credit Union to the University of Phoenix when he was a student.

763. As described herein, the Private Information of Plaintiff Wyche has already been published—or will be published imminently—by CL0P on the Dark Web.

764. In response to the risks created by the Data Breach, Plaintiff Wyche has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Wyche has lost approximately ten (10) hours researching the Data Breach, investigating fraud, contacting his bank, and monitoring his accounts for suspicious activity.

765. Because of the Data Breach, Plaintiff Wyche anticipates spending considerable amounts of time and money to try and mitigate his injuries.

766. In the aftermath of the Data Breach, Plaintiff Wyche suffered from a spike in suspicious spam and scam text messages and/or phone calls.

767. Plaintiff Wyche fears for his personal financial security and worries about what information was exposed in the Data Breach.

768. Because of the Data Breach, Plaintiff Wyche has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

769. Plaintiff Wyche suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

770. Plaintiff Wyche suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

771. As a former student, Plaintiff Wyche suffered actual injury and lost the "benefit of the bargain" because Plaintiff Wyche paid Defendants for services and reasonable data security—but Defendants then cut corners and declined to provide the bargained for data security. After all, if Defendants were transparent about its deficient data security, then Plaintiff Wyche (1) would have either declined to become a customer of Defendants and would have taken his business to a competitor of Defendants, or (2) would have become a customer Defendants only if Defendants reduced its prices to account for the deficient data security.

772. Plaintiff Wyche suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Wyche's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

773. Today, Plaintiff Wyche has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Sarah Clark

774. Plaintiff Sarah Clark is a former employee of the University of Phoenix.

775. The University of Phoenix required that Plaintiff Clark disclose her Private Information. Thus, the University of Phoenix obtained and maintained her Private Information.

776. On information and belief, the types of Private Information that the University of Phoenix obtained and maintained from Plaintiff Clark included her Social Security number, driver's license number, date of birth, name, address, email, phone, and other contact information.

777. On information and belief, the University of Phoenix disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

778. As a result, Plaintiff Clark was injured by the Data Breach.

779. Plaintiff Clark is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

780. Plaintiff Clark (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

781. Plaintiff Clark does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

782. Plaintiff Clark received a Notice of Data Breach from the University of Phoenix dated December 22, 2025.

783. Through their Data Breach, Defendants compromised Plaintiff Clark's Private Information.

784. Plaintiff Clark has ***already suffered*** from identity theft and fraud—wherein cybercriminals impersonated chase bank employees and contacted her falsely claiming that there were unauthorized charges to her financial accounts and accurately recited her Social Security number to her in an attempt to induce her to provide additional personal information. Ms. Clark terminated the call and reached out to Chase bank directly who informed her that no such charges were being attempted and that Chase had not attempted to contact her.

785. As described herein, the Private Information of Plaintiff Clark has already been published—or will be published imminently—by CL0P on the Dark Web.

786. In response to the risks created by the Data Breach, Plaintiff Clark has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Clark has lost several hours monitoring her accounts for suspicious activity, investigating fraudulent activity, and researching the Data Breach.

787. Because of the Data Breach, Plaintiff Clark anticipates spending considerable amounts of time and money to try and mitigate her injuries.

788. Plaintiff Clark fears for her personal financial security and worries about what information was exposed in the Data Breach.

789. Because of the Data Breach, Plaintiff Clark has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

790. Plaintiff Clark suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

791. Plaintiff Clark suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

792. As a former employee, Plaintiff Clark suffered actual injury and lost the "benefit of the bargain" when Plaintiff Clark (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Clark would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

793. Plaintiff Clark suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Clark's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

794. Today, Plaintiff Clark has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Anthony Bryant

795. Plaintiff Anthony Bryant is a current employee of the Washington Post.

796. The Washington Post required that Plaintiff Bryant disclose his Private Information. Thus, the Washington Post obtained and maintained his Private Information.

797. On information and belief, the types of Private Information that the Washington Post obtained and maintained from Plaintiff Bryant included his name, date of birth, address, Social Security number, employment information, and financial account information.

798. On information and belief, the Washington Post disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

799. As a result, Plaintiff Bryant was injured by the Data Breach.

800. Plaintiff Bryant is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

801. Plaintiff Bryant (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

802. Plaintiff Bryant reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

803. Plaintiff Bryant does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

804. Through their Data Breach, Defendants compromised Plaintiff Bryant's Private Information.

805. Plaintiff Bryant received a Notice of Data Breach from the Washington Post dated November 12, 2025. Therein, the Washington Post confirmed that the Data Breach exposed at least his "name, employee ID number, and bank account and routing number."

806. Plaintiff Bryant has ***already suffered*** from identity theft and fraud:

a. On September 12, 2025, at 5:54 PM, identity thieves placed a fraudulent charge for $84.95 on his debit card from Chime bank.

b. On September 12, 2025, at 5:59 PM, identity thieves placed another fraudulent charge for $144.95 on his debit card from Chime bank.

c. On September 24, 2025, at 9:12 AM, identity thieves placed another fraudulent charge for $200.00 on his debit card from Chime bank.

807. Notably, pursuant to his employment, Plaintiff had previously disclosed the account numbers for his Chime bank account to the Washington Post.

808. Furthermore, in the Data Breach notice that he received, the Washington Post specifically identified his Chime bank account as the "bank account number impacted by this incident[.]" Specifically, the Data Breach listed the last "four digits" of the impacted account which are the exact digits of his Chime bank account (i.e., "The bank account number impacted by this incident ends with these four digits [XXXX].").

809. As described herein, the Private Information of Plaintiff Bryant has already been published—or will be published imminently—by CL0P on the Dark Web.

810. In response to the risks created by the Data Breach, Plaintiff Bryant has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Bryant has lost approximately twenty (20) hours researching the data breach, contacting credit bureaus to freeze his credit, investigating the fraud, calling the Data Breach hotline to confirm his exposure, contacting his bank, and monitoring his accounts for suspicious activity.

811. Because of the Data Breach, Plaintiff Bryant anticipates spending considerable amounts of time and money to try and mitigate his injuries.

812. In the aftermath of the Data Breach, Plaintiff Bryant suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

813. Plaintiff Bryant fears for his personal financial security and worries about what information was exposed in the Data Breach.

814. Because of the Data Breach, Plaintiff Bryant has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

815. Plaintiff Bryant suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

816. Plaintiff Bryant suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

817. As a current employee, Plaintiff Bryant suffered actual injury and lost the "benefit of the bargain" when Plaintiff Bryant (or his third-party agent) provided his labor to Defendants

in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Bryant would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

818. Plaintiff Bryant suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Bryant's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

819. Today, Plaintiff Bryant has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Bruce Bennett

820. Plaintiff Bruce Bennett is a former employee of the Washington Post.

821. The Washington Post required that Plaintiff Bennett disclose his Private Information. Thus, the Washington Post obtained and maintained his Private Information.

822. On information and belief, the types of Private Information that the Washington Post obtained and maintained from Plaintiff Bennett included his name, contact information, Social Security number, and financial account information.

823. On information and belief, the Washington Post disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

824. As a result, Plaintiff Bennett was injured by the Data Breach.

825. Plaintiff Bennett is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe

manner. He is careful to store any documents containing his Private Information in a secure location.

826. Plaintiff Bennett (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

827. Plaintiff Bennett reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

828. Plaintiff Bennett does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

829. Plaintiff Bennett received a Notice of Data Breach from the Washington Post dated November 12, 2025. Therein, the Washington Post confirmed that the Data Breach exposed at least his "name, employee ID number, and bank account and routing number."

830. Through their Data Breach, Defendants compromised Plaintiff Bennett's Private Information.

831. As described herein, the Private Information of Plaintiff Bennett has already been published—or will be published imminently—by CL0P on the Dark Web.

832. In response to the risks created by the Data Breach, Plaintiff Bennett has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Bennett has lost approximately ten (10) hours

researching the Data Breach, contacting credit bureaus, contacting his bank, and monitoring his accounts for suspicious activity.

833. Because of the Data Breach, Plaintiff Bennett anticipates spending considerable amounts of time and money to try and mitigate his injuries.

834. In the aftermath of the Data Breach, Plaintiff Bennett suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

835. Plaintiff Bennett fears for his personal financial security and worries about what information was exposed in the Data Breach.

836. Because of the Data Breach, Plaintiff Bennett has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

837. Plaintiff Bennett suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

838. Plaintiff Bennett suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

839. As a former employee, Plaintiff Bennett suffered actual injury and lost the "benefit of the bargain" when Plaintiff Bennett (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Bennett would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

840. Plaintiff Bennett suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Bennett's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

841. Today, Plaintiff Bennett has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff James Nance

842. Plaintiff James Nance is a former employee of the Washington Post.

843. The Washington Post required that Plaintiff Nance disclose his Private Information. Thus, the Washington Post obtained and maintained his Private Information.

844. On information and belief, the types of Private Information that the Washington Post obtained and maintained from Plaintiff Nance included his name, date of birth, contact information, Social Security number, financial account information, and insurance information.

845. On information and belief, the Washington Post disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

846. As a result, Plaintiff Nance was injured by the Data Breach.

847. Plaintiff Nance is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

848. Plaintiff Nance (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal

policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

849. Plaintiff Nance reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

850. Plaintiff Nance does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

851. Plaintiff Nance received a Notice of Data Breach from the Washington Post dated November 12, 2025.

852. Through their Data Breach, Defendants compromised Plaintiff Nance's Private Information.

853. As described herein, the Private Information of Plaintiff Nance has already been published—or will be published imminently—by CL0P on the Dark Web.

854. In response to the risks created by the Data Breach, Plaintiff Nance has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Nance has lost approximately six (6) hours researching the Data Breach, contacting his bank, and monitoring his accounts for suspicious activity.

855. Because of the Data Breach, Plaintiff Nance anticipates spending considerable amounts of time and money to try and mitigate his injuries.

856. Since August 2025, Plaintiff Nance suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

857. Plaintiff Nance fears for his personal financial security and worries about what information was exposed in the Data Breach.

858. Because of the Data Breach, Plaintiff Nance has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

859. Plaintiff Nance suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

860. Plaintiff Nance suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

861. As a former employee, Plaintiff Nance suffered actual injury and lost the "benefit of the bargain" when Plaintiff Nance (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Nance would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

862. Plaintiff Nance suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Nance's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

863. Today, Plaintiff Nance has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Rachel Hatzipanagos

864. Plaintiff Rachel Hatzipanagos is a current employee of the Washington Post.

865. The Washington Post required that Plaintiff Hatzipanagos disclose her Private Information. Thus, the Washington Post obtained and maintained her Private Information.

866. On information and belief, the types of Private Information that the Washington Post obtained and maintained from Plaintiff Hatzipanagos included her name, date of birth, Social Security number, contact information, financial account information (for direct deposit), address, and driver's license information.

867. On information and belief, the Washington Post disclosed her Private Information to Oracle by inputting her Private Information into Oracle EBS.

868. As a result, Plaintiff Hatzipanagos was injured by the Data Breach.

869. Plaintiff Hatzipanagos is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

870. Plaintiff Hatzipanagos (or her third-party agent) provided her Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain her Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

871. Plaintiff Hatzipanagos reasonably understood that a portion of the funds paid to Defendants (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of Private Information.

872. Plaintiff Hatzipanagos received a Notice of Data Breach from the Washington Post.

873. Through their Data Breach, Defendants compromised Plaintiff Hatzipanagos's Private Information.

874. As described herein, the Private Information of Plaintiff Hatzipanagos has already been published—or will be published imminently—by CL0P on the Dark Web.

875. In response to the risks created by the Data Breach, Plaintiff Hatzipanagos has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. Specifically, Plaintiff Hatzipanagos has lost approximately five (5) hours researching the Data Breach, contacting credit bureaus, researching her legal options, and monitoring her accounts for suspicious activity.

876. Because of the Data Breach, Plaintiff Hatzipanagos anticipates spending considerable amounts of time and money to try and mitigate her injuries.

877. In the aftermath of the Data Breach, Plaintiff Hatzipanagos suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

878. Plaintiff Hatzipanagos fears for her personal financial security and worries about what information was exposed in the Data Breach.

879. Because of the Data Breach, Plaintiff Hatzipanagos has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

880. Plaintiff Hatzipanagos suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy and warrants, at minimum, nominal damages.

881. Plaintiff Hatzipanagos suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

882. As a current employee, Plaintiff Hatzipanagos suffered actual injury and lost the "benefit of the bargain" when Plaintiff Hatzipanagos (or her third-party agent) provided her labor to Defendants in exchange for both payment and reasonable data security for her Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Hatzipanagos would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

883. Plaintiff Hatzipanagos suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Hatzipanagos's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

884. Today, Plaintiff Hatzipanagos has a continuing interest in ensuring that her Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Richard Leiby

885. Plaintiff Richard Leiby is a former employee of the Washington Post.

886. The Washington Post required that Plaintiff Leiby disclose his Private Information. Thus, the Washington Post obtained and maintained his Private Information.

887. On information and belief, the types of Private Information that the Washington Post obtained and maintained from Plaintiff Leiby included his name, Social Security number, and financial account information (including bank account number and routing number).

888. On information and belief, the Washington Post disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

889. As a result, Plaintiff Leiby was injured by the Data Breach.

890. Plaintiff Leiby is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

891. Plaintiff Leiby (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

892. Plaintiff Leiby reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

893. Plaintiff Leiby does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

894. Plaintiff Leiby received a Notice of Data Breach from the Washington Post dated November 12, 2025.

895. Through their Data Breach, Defendants compromised Plaintiff Leiby's Private Information.

896. Plaintiff Leiby has ***already suffered*** from identity theft and fraud—whereby cybercriminals placed fraudulent charges on his debit card for train tickets and cruise tickets totaling approximately $900 on or around August 2025.

897. As described herein, the Private Information of Plaintiff Leiby has already been published—or will be published imminently—by CL0P on the Dark Web.

898. In response to the risks created by the Data Breach, Plaintiff Leiby has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Leiby has lost approximately three (3) hours researching the Data Breach, contacting his bank, and monitoring his accounts for suspicious activity.

899. Because of the Data Breach, Plaintiff Leiby anticipates spending considerable amounts of time and money to try and mitigate his injuries.

900. In the aftermath of the Data Breach, Plaintiff Leiby suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls.

901. Plaintiff Leiby fears for his personal financial security and worries about what information was exposed in the Data Breach.

902. Because of the Data Breach, Plaintiff Leiby has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

903. Plaintiff Leiby suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

904. Plaintiff Leiby suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

905. As a former employee, Plaintiff Leiby suffered actual injury and lost the "benefit of the bargain" when Plaintiff Leiby (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Leiby would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

906. Plaintiff Leiby suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Leiby's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

907. Today, Plaintiff Leiby has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

Plaintiff Jun Hee Kim

908. Plaintiff Jun Hee Kim is a former employee of the Washington Post.

909. The Washington Post required that Plaintiff Kim disclose his Private Information. Thus, the Washington Post obtained and maintained his Private Information.

910. On information and belief, the types of Private Information that the Washington Post obtained and maintained from Plaintiff Kim included his name, date of birth, contact information, Social Security number, financial account information, and insurance information.

911. On information and belief, the Washington Post disclosed his Private Information to Oracle by inputting his Private Information into Oracle EBS.

912. As a result, Plaintiff Kim was injured by the Data Breach.

913. Plaintiff Kim is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

914. Plaintiff Kim (or his third-party agent) provided his Private Information to Defendants and trusted they would use reasonable measures to protect it according to their internal policies, as well as state and federal law. Defendants obtained and continue to maintain his Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

915. Plaintiff Kim reasonably understood that a portion of the funds paid to Defendants (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of Private Information.

916. Plaintiff Kim does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

917. Plaintiff Kim received a Notice of Data Breach from the Washington Post dated November 12, 2025.

918. Through their Data Breach, Defendants compromised Plaintiff Kim's Private Information.

919. As described herein, the Private Information of Plaintiff Kim has already been published—or will be published imminently—by CL0P on the Dark Web.

920. In response to the risks created by the Data Breach, Plaintiff Kim has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Specifically, Plaintiff Kim has lost approximately six (6) hours verifying the legitimacy of the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts and continues to spend time changing his passwords, and checking his financial accounts for a minimum of an hour per week.

921. Because of the Data Breach, Plaintiff Kim anticipates spending considerable amounts of time and money to try and mitigate his injuries.

922. Since the Data Breach, Plaintiff Kim suffered from a spike in suspicious spam and scam emails, text messages and/or phone calls. He receives at least one spam call or text message every day.

923. Plaintiff Kim fears for his personal financial security and worries about what information was exposed in the Data Breach.

924. Because of the Data Breach, Plaintiff Kim has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

925. Plaintiff Kim suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy and warrants, at minimum, nominal damages.

926. Plaintiff Kim suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

927. As a former employee, Plaintiff Kim suffered actual injury and lost the "benefit of the bargain" when Plaintiff Kim (or his third-party agent) provided his labor to Defendants in exchange for both payment and reasonable data security for his Private Information. After all, if Defendants were transparent about its deficient data security, then Plaintiff Kim would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

928. Plaintiff Kim suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because the Data Breach placed Plaintiff Kim's Private Information right in the hands of the Russian cybercriminal syndicate CL0P.

929. Today, Plaintiff Kim has a continuing interest in ensuring that his Private Information—which, upon information and belief, is still negligently stored by Defendants—is protected and safeguarded from additional breaches.

VI. COMMON ALLEGATIONS

Consumers Prioritize Data Security

930. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[191] Therein, Cisco reported the following:

[191] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[192]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[193]

c. 89% of consumers stated that "I care about data privacy."[194]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[195]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[196]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[197]

Plaintiffs and the Proposed Class Suffered Common Injuries and Damages

931. Because of Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

---

[192] *Id*. at 3.
[193] *Id*.
[194] *Id*. at 9.
[195] *Id*.
[196] *Id*.
[197] *Id*. at 11.

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identity theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information—which remains in Defendants' possession—and is thus at risk for futures breaches so long as Defendants fails to take appropriate measures to protect the Private Information.

932. As former employees of some of the Defendants, relevant Plaintiffs and relevant Class Members suffered actual injury and lost the "benefit of the bargain" when they (or their third-party agent) provided their labor to the relevant Defendants in exchange for both payment and reasonable data security for their Private Information. After all, if the relevant Defendants were transparent about their deficient data security, relevant Plaintiffs and relevant Class Members would have either (1) not worked for Defendants at all, or (2) would have required a salary premium (i.e., a "compensating wage differential") to account for the non-standard risk incurred.

Substantially Increased Risk of Identity Theft and Fraud

933. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

934. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

935. 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 "[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." *Id*.

936. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market (aka the Dark Web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

937. The "Dark Web" is an unindexed layer of the internet that requires special software or authentication to access.[198] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[199] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

938. The unencrypted Private Information of Plaintiffs and Class Members has or will end up for sale on the Dark Web because that is the modus operandi of hackers, particularly here,

[198] *What Is the Dark Web?*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-isthe-dark-web/ (last visited July 9, 2025).
[199] *Id*.

where the Private Information was targeted by a ransomware group known to trade in Private Information. In addition, the unencrypted and detailed Private Information, already published on the Dark Web may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can now easily access the Plaintiffs' and Class Members' Private Information.

939. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

940. In particular, the theft of Social Security numbers—in combination with other Private Information (e.g., name, address, date of birth)—provides cybercriminals with a "skeleton key" to commit rampant fraud and identity theft.

941. For example, cybersecurity expert Jim Stickley explained to Time Magazine that "[i]f I have your name and your Social Security number, and you haven't gotten a credit freeze yet, you're easy pickings . . . With that, you can do whatever you want . . . You can become that person."[200] For context, Jim Stickley is a "penetration tester" who is employed by businesses "to infiltrate their systems in order to find flaws they can fix before the bad guys exploit them."[201]

942. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even

[200] Patrick L. Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME MAGAZINE (Aug. 5, 2019) https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[201] *Id*.

years, later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

943. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[202]

944. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

945. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

946. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

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

through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

947. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that victims lost approximately $18.7 million to such scams in 2023 alone.[203]

948. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[204]

949. One example of criminals piecing together bits and pieces of compromised Private Information to create comprehensive dossiers on individuals is called "Fullz" packages.[205] These

[203] *Internet Crime Report*, FEDERAL BUREAU OF INVESTIGATION, (2023), https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf scams.

[204] *Identity Theft and Your Social Security Number,* SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited July 9, 2025).

[205] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account)

dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. For example, they can combine the stolen Private Information, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

950. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

951. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[206]

---

without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm,* KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

[206] *2019 Internet Crime Report* (Feb. 11, 2020) FED. BUREAU INTELLIGENCE, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

952. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Yet, Defendants failed to rapidly report to Plaintiffs and the Class that their Private Information was stolen. Defendants' failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

953. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

954. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

955. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

Defendants Knew—Or Should Have Known—of the Risk of a Data Breach

956. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

957. In 2024, a record 3,158 data breaches occurred—exposing approximately

1,350,835,988 sensitive records (i.e., 211% increase year over year).[207]

958. In light of high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendants knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

959. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants themselves. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[208]

960. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

Defendants Could Have Prevented the Data Breach

961. Data breaches are preventable.[209] Indeed, the American Bar Association published a treatise titled the *Data Breach and Encryption Handbook* wherein the author explained that:

a. "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[210]

---

[207] *2024 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.
[208] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach
[209] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (2012).
[210] *Id.* at 17.

b. "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[211]

c. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs." [212]

Defendants Failed to Follow FTC Guidelines

962. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

963. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[213] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

[211] *Id.* at 28.
[212] *Id.*
[213] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

e. implement policies to correct security problems.

964. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

965. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

966. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

967. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to the data of their current and former employees, contractors, and patients constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

968. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

969. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

970. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

971. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

VII. CLASS ACTION ALLEGATIONS

972. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following nationwide class (the "Class"):

> All individuals residing in the United States whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

973. Plaintiffs also propose the following Arizona subclass (the "Arizona Subclass"), to be represented by Plaintiffs Mosby and Bennett:

> All individuals residing in Arizona whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

974. Plaintiffs also propose the following California subclass (the "California Subclass"), to be represented by Plaintiffs Koyfman, Eagan, Alvarado, and Gilula:

> All individuals residing in California whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

975. Plaintiffs also propose the following Colorado subclass (the "Colorado Subclass"), to be represented by Plaintiff Nance:

> All individuals residing in Colorado whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

976. Plaintiffs also propose the following Connecticut subclass (the "Connecticut Subclass"), to be represented by Plaintiff Nero:

> All individuals residing in Connecticut whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

977. Plaintiffs also propose the following District of Columbia subclass (the "D.C. Subclass"), to be represented by Plaintiff Leiby:

> All individuals residing in the District of Colombia whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

978. Plaintiffs also propose the following Georgia subclass (the "Georgia Subclass"), to be represented by Plaintiff Wyche:

> All individuals residing in Georgia whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

979. Plaintiffs also propose the following Illinois subclass (the "Illinois Subclass"), to be represented by Plaintiffs Ranson and Pointer:

> All individuals residing in Illinois whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

980. Plaintiffs also propose the following Maryland subclass (the "Maryland Subclass"), to be represented by Plaintiffs Kim, Naulty, and Hatzipanagos:

> All individuals residing in Maryland whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

981. Plaintiffs also propose the following Massachusetts subclass (the "Massachusetts Subclass"), to be represented by Plaintiffs Youmell and Ross:

> All individuals residing in Massachusetts whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

982. Plaintiffs also propose the following Michigan subclass (the "Michigan Subclass"), to be represented by Plaintiff Clark:

> All individuals residing in Massachusetts whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

983. Plaintiffs also propose the following New Jersey subclass (the "New Jersey Subclass"), to be represented by Plaintiff Liranzo:

> All individuals residing in New Jersey whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

984. Plaintiffs also propose the following New Hampshire subclass (the "New Hampshire Subclass"), to be represented by Plaintiff Mabey:

> All individuals residing in New Hampshire whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

985. Plaintiffs also propose the following New York subclass (the "New York Subclass"), to be represented by Plaintiffs Brown, Yao, and Sainvil:

> All individuals residing in New York whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

986. Plaintiffs also propose the following North Carolina subclass (the "North Carolina Subclass"), to be represented by Plaintiff Trempus:

> All individuals residing in North Carolina whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

987. Plaintiffs also propose the following Oklahoma subclass (the "Oklahoma Subclass"), to be represented by Plaintiff Boggs:

> All individuals residing in Oklahoma whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

988. Plaintiffs also propose the following Texas subclass (the "Texas Subclass"), to be represented by Plaintiffs Magnusson, Tannehill, Issac, O'Keeffe, and Vega:

> All individuals residing in Texas whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

989. Plaintiffs also propose the following Virginia subclass (the "Virginia Subclass"), to be represented by Plaintiffs Massengill and Bryant:

> All individuals residing in Virginia whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

990. Plaintiffs also propose the following Washington subclass (the "Washington Subclass"), to be represented by Plaintiff Reynolds:

> All individuals residing in Washington whose Private Information was compromised in the Data Breach that impacted Oracle EBS in or around July 2025, including all those individuals who received notice of the breach.

991. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants has a controlling interest, any Defendants'ff officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

992. Plaintiffs reserve the right to amend the class definition.

993. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

994. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendants' custody and control. After all, Defendants already identified some individuals and sent them data breach notices.

995. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least one million members.

996. Typicality. Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

997. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

998. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendants had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Private Information;

b. if Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendants were negligent in maintaining, protecting, and securing Private Information;

d. if Defendants breached contract promises to safeguard Plaintiffs and the Class's Private Information;

e. if Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendants' Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

999. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

VIII. CAUSES OF ACTION

Count I – Negligence

1000. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

1001. This claim is brought:

a. by all Plaintiffs on behalf of the nationwide Class; or

b. or alternatively by relevant Plaintiffs on behalf of the subclasses for: Arizona, California, Colorado, Connecticut, District of Columbia, Georgia, Illinois, Maryland, Massachusetts, Michigan, New Jersey, New Hampshire, New York, North Carolina, Oklahoma, Texas, Virginia, Washington.

1002. Plaintiffs and the Class (or their third-party agents) entrusted their Private Information to Defendants on the premise and with the understanding that Defendants would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

1003. Plaintiffs and Class Members relied on Defendants to exercise discretion and professional judgment in securing their Private Information and Plaintiffs and Class Members had no way to audit, influence, or verify the integrity of Defendants data security practices. Defendants were in an exclusive position to protect against the Data Breach.

1004. Defendants owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendants' failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

1005. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

1006. Defendants owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security practices. After all, Defendants actively sought and obtained Plaintiffs and Class Members' Private Information.

1007. Defendants owed—to Plaintiffs and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in their care and custody;

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

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

1008. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

1009. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain under applicable regulations or circumstances.

1010. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

1011. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third-party agents) entrusted Defendants with their confidential Private Information, a necessary part of obtaining services from Defendant.

1012. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

1013. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs and the Class Members' sensitive Private Information.

1014. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information Defendants had collected and stored and the

foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

1015. Similarly, and as described *infra*, Defendants violated their duties under the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA") the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*. (the "CRA"), and other state data security laws which constitutes negligence.

1016. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Private Information —whether by malware or otherwise.

1017. Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members' and the importance of exercising reasonable care in handling it.

1018. Defendants improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

1019. Defendants breached these duties as evidenced by the Data Breach.

1020. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

1021. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs and Class Members' injury.

1022. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' injuries-in-fact.

1023. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

1024. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

1025. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

1026. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants'

negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

Count II – Invasion of Privacy

1027. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

1028. This claim is brought by relevant Plaintiffs on behalf of the subclasses for: Arizona, California, Colorado, Connecticut, District of Columbia, Georgia, Illinois, Maryland, Massachusetts, Michigan, New Jersey, New Hampshire, North Carolina, Oklahoma, Texas, Virginia, Washington.

1029. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

1030. Defendants owed a duty to their current and former employees, contractors, students, and/or customers including Plaintiffs and the Class, to keep this information confidential.

1031. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' Private Information is highly offensive to a reasonable person.

1032. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

1033. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

1034. Defendants acted with a knowing state of mind when it permitted the Data Breach because it knew their information security practices were inadequate.

1035. Defendants acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

1036. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

1037. As a proximate result of Defendants' acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

1038. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

1039. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information are still maintained by Defendants with their inadequate cybersecurity system and policies.

1040. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for

monetary damages will not end Defendants' inability to safeguard the Private Information of Plaintiffs and the Class.

1041. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

Count III – Violations of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150

1042. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

1043. This claim is brought against Defendants Oracle, MSG, and University of Pennsylvania by Plaintiffs Koyfman, Eagan, Alvarado, and Gilula on behalf of a nationwide Class and/or the California Subclass.

1044. Defendants Oracle, MSG, and University of Pennsylvania violated the California Consumer Privacy Act ("CCPA") by providing overly delayed notice whereas the CCPA requires disclosure "within 30 calendar days of discovery or notification of the data breach." Cal. Civ. Code § 1798.82(a)(2)(A).

1045. Defendants Oracle, MSG, and University of Pennsylvania violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiffs Koyfman, Eagan, Alvarado, and Gilula and the California Subclass. As a direct and proximate result, Plaintiffs' and the California Subclass's nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

1046. Defendants Oracle, MSG, and University of Pennsylvania are each a "business" under the meaning of Civil Code § 1798.140 because Defendants are each a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civ. Code § 1798.140(d).

1047. Plaintiffs Koyfman, Eagan, Alvarado, and Gilula and California Subclass Members seek injunctive or other equitable relief to ensure Defendants Oracle, MSG, and University of Pennsylvania hereinafter adequately safeguard Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants Oracle, MSG, and University of Pennsylvania continue to hold Private Information, including Plaintiffs' and California Subclass Members' Private Information. Plaintiffs and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

1048. Pursuant to California Civil Code § 1798.150(b), Plaintiffs will provide notice to Defendants and amend to seek statutory damages if Defendants are unable to cure the identified deficiencies within thirty (30) days. Thus, Plaintiffs presently seek only actual damages under CCPA.

1049. As described herein, an actual controversy has arisen and now exists as to whether Defendants Oracle, MSG, and University of Pennsylvania implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

1050. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants Oracle, MSG, and University of Pennsylvania.

Count IV– Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.

1051. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

1052. This claim is brought against Defendants Oracle and University of Pennsylvania by Plaintiff Gilula on behalf of the California Subclass.

1053. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, ***or*** is reasonably believed to have been, acquired by an unauthorized person." *Id* (emphasis added).

1054. The Data Breach constitutes a "breach of the security system" of Defendants Oracle and University of Pennsylvania.

1055. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the California Subclass.

1056. Defendants Oracle and University of Pennsylvania knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the California Subclass but notified them after an unreasonable delay.

1057. Defendants' unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

1058. Because Plaintiffs and the California Subclass were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

1059. Plaintiffs and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

IX. PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendants and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendants from further unfair and/or deceptive practices;

E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, nominal damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

X. DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: March 6, 2026

Respectfully submitted,

By: */s/ W. Mark Lanier*

W. Mark Lanier
Texas Bar No. 11934600
LANIER LAW FIRM
10940 W. Sam Houston Pkwy N., Suite 100
Houston, TX 77064
Tel: 713-659-5200
Mark.Lanier@lanierlawfirm.com

Gary Klinger
Bar No. 6303726
MILBERG, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-252-0878
gklinger@milberg.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: 954-332-2100
ostrow@kolawyers.com

Interim Co-Lead Class Counsel

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Tel: 214/744-3000
jkendall@kendalllawgroup.com

Interim Liaison Counsel

James Pizzirusso*
HAUSFELD LLP
1200 17th Street, NW, Suite 600
Washington, DC 20036
Tel: 202-540-7200
jpizirusso@hausfeld.com

Tom Loeser
COTCHETT, PITRE & MCCARTHY LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: 206.802.1272
tloeser@cpmlegal.com

Raina Borrelli*
STRAUSS BORELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: 872-263-1100
raina@straussborrelli.com

Leigh Montgomery
Texas Bar No. 24052214
ELLZEY KHERKHER SANFORD MONTGOMERY, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Tel: 888-350-3931
lmontgomery@eksm.com
Service only: service@eksm.com

J. Gerard Stranch, IV*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parkes Avenue, Suite 200
Nashville, TN 37203
Tel: 615-254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Lynn A. Toops*
Amina A. Thomas*
COHENMALAD LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
Tel: 317-636-6481
ltoops@cohenmalad.com
athomas@cohenamalad.com

William B. Federman
Tex. Bar No. 00794935
Jessica W. Wilkes
FEDERMAN & SHERWOOD
4131 N. Central Expressway, Ste. 900
Dallas, TX 75204
Tel: (800) 237-1277
wbf@federmanlaw.com
jaw@federmanlaw.com

David C. Lawrence
Texas Bar No. 24041304
Braden N. Anderson
Texas Bar No. 24138083
RIGBY SLACK PLLC
3500 Jefferson Street, Suite 330
Austin, Texas 78731
Tel: 512-782-2060
dlawrence@rigbyslack.com
banderson@rigbyslack.com

Scott Falgoust
BRYSON HARRIS SUCIU DEMAY PLLC
5301 Canal Boulevard
New Orleans, LA 70124
Tel: (844) 201-2929
sfalgoust@brysonpllc.com

Paul Doolittle (*pro hac vice*)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Tel: 803-222-2222
paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Sabita J. Soneji
TYCKO & ZAVAREEI LLP
19700 Broadway, Suite 1070
Oakland, CA 94612
Tel.: (510) 254-6808
ssoneji@tzlegal.com

Executive Committee

**Pro hac vice forthcoming*
Attorneys for Plaintiffs and Proposed Class

CERTIFICATE OF SERVICE

I, the undersigned, hereby certify that a true and correct copy of the foregoing instrument was filed using the Court's CM/ECF system on March 6, 2026, which will deliver electronic notice of same to all counsel of record.

Date: March 6, 2026

Respectfully submitted,

By: */s/ W. Mark Lanier*
W. Mark Lanier

— EXHIBIT A —

SUNY RF
The Research Foundation for The State University of New York

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Richard Yao
[redacted]

January 29, 2026

Dear Richard Yao:

The Research Foundation for The State University of New York ("RF SUNY") is writing to notify you of a data security incident that involved our third-party vendor, Oracle. This notice explains the incident, measures we have taken, and steps you can take in response.

On October 10, 2025, RF SUNY learned that unauthorized parties exploited a zero-day vulnerability in Oracle's E-Business Suite application, which RF SUNY uses to maintain business information, including human resources and benefits-related information. RF SUNY took the Oracle's E-Business Suite application offline, applied software patches provided by Oracle, notified law enforcement, and launched an investigation. Through our investigation, on October 13, 2025, RF SUNY determined that the vulnerability in the Oracle's E-Business Suite application allowed unauthorized parties to access and acquire files stored in the application between August 9 and 11, 2025.

As part of the ongoing investigation, RF SUNY worked diligently to identify the files that were subject to unauthorized access / acquisition as a result of the vulnerability in Oracle's E-Business Suite application. On November 26, 2025, RF SUNY determined one or more files contained your name and Social Security number.

We have secured the services of Experian® to offer you a complimentary one-year membership of Experian's IdentityWorks℠. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary membership, as well as some additional steps you can take, please see the pages that follow this letter.**

To help prevent something like this from happening in the future, RF SUNY is working to ensure that Oracle and other third-party providers deliver secure, compliant software and services, including the timely identification of vulnerabilities and execution of remediation plans.

If you have any questions about this incident, please call 855-815-3916, Monday through Friday, between 9:00 a.m. and 9:00 p.m., Eastern Time.

Sincerely,

The Research Foundation for The State University of New York

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: $750K Settlement Resolves Claims Against Dartmouth in Class Action Lawsuit Tied to Massive Oracle Data Breach