Kristen Lake Cardoso (SBN 338762)
cardoso@kolawyers.com
KOPELOWITZ OSTROW P.A.
One W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Telephone: (954) 990-2218

[Additional Counsel in Signature Block]

Attorney for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

GANESH SANKAR, ERIKA TITUS-LAY, JARED CAVANAUGH, and KIMBERLY VONGNALITH, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

CALIFORNIA NORTHSTATE UNIVERSITY, LLC,

Defendant.

Lead Case: 2:24-cv-00473-DAD-JDP
Member Case: 2:24-cv-01231-DAD-JDP

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Ganesh Sankar, Erika Titus-Lay, Jared Cavanaugh, and Kimberly Vongnalith, (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint ("Complaint") against Defendant California Northstate University, LLC ("Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the recent targeted ransomware attack and data breach ("Data Breach") on Defendant's network that resulted in unauthorized access to the highly sensitive data. As a result of the Data Breach, Class Members (defined *infra*) suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably

incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. The specific information compromised in the Data Breach includes, but is not limited to, personally identifiable information ("PII"), such as full names and Social Security numbers.

3. Up to and through February 2024, Defendant obtained the PII of Plaintiffs and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network, from which unauthorized actors used an extraction tool to retrieve sensitive PII belonging to Plaintiffs and Class Members.

4. Plaintiffs' and Class Members' PII—which were entrusted to Defendant, their officials, and agents—were compromised and unlawfully accessed due to the Data Breach.

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiffs' and Class Members' PII.

8. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiffs and Class Members will remain for their respective

lifetimes.

9. Defendant failed to provide timely, accurate and adequate notice to Plaintiffs and Class Members. Plaintiffs' and Class Members' knowledge about the PII Defendant lost, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

10. As remediation for allowing Plaintiffs' and Class Members' PII to be acquired by an unauthorized third-party, Defendant has stated that "[w]e are offering you a complimentary one-year membership to Experian's IdentityWorks."[1]

11. Indeed, armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present, heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

13. Plaintiffs and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

15. Accordingly, Plaintiffs bring claims on behalf of themselves and the Class for: (i) negligence, (ii) invasion of privacy (iii) unjust enrichment, (iv) violations of the California Unfair

[1] *See, e.g.*, Notice of Breach letter to Plaintiff Sankar, attached hereto as **Exhibit A**.

Competition Law, (v) violation of the California Consumer Privacy Act, (vi) violation of the California Customer Records Act and (vii) declaratory judgment and injunctive relief. Through these claims, Plaintiffs seek, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

16. Plaintiff Sankar is a natural person and citizen of Georgia.

17. Plaintiff Titus-Lay is a natural person and citizen of California.

18. Plaintiff Jared Cavanaugh is a natural person and citizen of California.

19. Plaintiff Kimberly Vongnalith is a natural person and citizen of California.

20. Defendant is a limited liability company formed in Delaware and registered in good standing in California. According to the California Secretary of State, Defendant's California Registered Corporate Agents are Amanda Garcia, Gabriela Sanchez, Daisy Montenegro, Beatrice Casarez-Barrientez, Jessie Gastelum, John Montijo, Diana Ruiz, Sarai Marin, Emanuel Jacobo, Gladys Aguilera, Vivian Imperial, Carlos Paz, Alberto Damonte, Peter Cayetano, Elsa Montanez, Xenia Perez, Yesenia Carpenter, and Jaqueline Mejia, who, upon information and belief, are citizens of California.

JURISDICTION AND VENUE

21. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, including Plaintiff Sankar, are citizens of a different state than Defendant, and the amount in controversy exceeds $5 million exclusive of interest and costs.

22. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and this District.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business is in this District and a substantial part of the events, acts, and omissions

giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND FACTS

A. Defendant's Businesses

24. Defendant is an institution dedicated to educating, developing and training individuals to provide competent, patient-centered care.[2]

25. On information and belief, Defendant maintains the PII of current, former, prospective students and employees, including but not limited to their:

a. names;

b. Social Security numbers and;

c. other information that Defendant may deem necessary to provide its services.

26. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

27. Because of the highly sensitive and personal nature of the information Defendant acquires, stores, and has access to, Defendant, upon information and belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

30. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained,

[2] *About the University*, CAL. NORTHSTATE UNIV., https://www.cnsu.edu/about/ (last visited June 10, 2024).

to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

31. Defendant recognizes that it owes duties to protect Plaintiffs' and Class Members' PII. For example, in its "Privacy Policy," Defendant promises that:

a. "We do not share your Personal Data with third parties except as described in this Policy or as otherwise disclosed to you on our Sites."[3]

b. "We take reasonable measures to protect Personal Data and other information we may receive from you in an effort to prevent loss, misuse and unauthorized access, disclosure, alteration, and destruction of such information."[4]

c. "[O]ur specific data handling practices and guidelines [] protect the security and confidentiality of your personal data."[5]

d. "We keep your information for as long as needed to fulfill the particular purpose for which it was collected."[6]

e. "Unless otherwise required by law, CNU will also erase Personal Data when it is no longer necessary[.]"[7]

f. "All reasonable steps will be taken to protect your privacy in accordance with all applicable data protection laws."[8]

32. Similarly, on its "Student Privacy" website, Defendant promises that: "The university does not disclose social security numbers, student or personal identification numbers . . . unless the student has signed a consent form."[9]

33. And again, in a separate "Privacy Policy," Defendant promises that:

a. "California Northstate University (CNU) follows industry guidelines for Privacy of and Access to Information, Electronic Information Security, and

---

[3] *Privacy Policy*, CAL. NORTHSTATE UNIV. (Dec. 5, 2020) https://www.cnsu.edu/privacy/.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Student Privacy*, CAL. NORTHSTATE UNIV., https://cnsu.edu/registrar/ferpa.php (last visited June 10, 2024).

Electronic Communications Policy, regarding the use of computer resources for the protection of all users."[10]

b. "Respect for the privacy of others is an important component of our University's policy and guidelines."[11]

c. "We do not share our registrants' information with other institutions, except as may be required by law."[12]

d. "We do not store credit card numbers on our servers."[13]

e. "We have appropriate security measures in place in our physical facilities to protect against the loss, misuse or alteration of information that we have collected from you."[14]

B. Defendant Fails to Safeguard Consumer PII

34. On or about December 21, 2023, Defendant began notifying current, former, and prospective students and employees of the Data Breach, informing them by a Notice of Breach letter:

> **What Happened?**
>
> [Defendant] recently completed its investigation of an incident that involved unauthorized access to certain University computer systems. Upon identifying the incident, we immediately secured the systems involved and began an investigation. Through the investigation we determined that between February 12, 2023 and February 13, 2023, an unauthorized actor potentially accessed and obtained certain files stored on our servers.
>
> **What Information Was Involved?**
>
> We reviewed the files that were potentially involved and on November 2, 2023, we identified one or more file(s) containing your name in combination with your Social Security number.
>
> **What You Can Do:**
>
> We are offering complimentary one-year membership to 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

[10] *Privacy Policy*, CAL. NORTHSTATE UNIV., https://medicine.cnsu.edu/lcme/privacy/ (last visited June 10, 2024).
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*

> identity theft. IdentityWorks is free and enrolling in this program will not affect your credit score. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership and steps you can take to protect your information, please see the pages that follow this letter.[15]

35. To be clear, Defendant waited ***ten months*** to inform Plaintiffs and Class Members that their PII had been compromised.

36. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiffs and the Class Members.

37. Plaintiffs further believe their PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

38. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

39. Because of the Data Breach, data thieves were able to gain access to Defendant's private systems between February 12, 2023, and February 13, 2023, and were able to compromise, access, and acquire the protected PII of Plaintiffs and Class Members.

40. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

41. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

42. Plaintiffs' and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The risks to Plaintiffs and Class Members will remain for

[15] *See* Exhibit A; *see also Notice of Data Breach*, CAL. ATTY GEN, https://oag.ca.gov/system/files/CNSU%20-%20California%20Notification.pdf (last visited June 10, 2024).

their respective lifetimes.

43. Worryingly, the cybercriminals that obtained Plaintiffs' and Class Members' PII appear to be the notorious cybercriminal group "AvosLocker."[16]

44. AvosLocker is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about AvosLocker. Specifically, the "Cybersecurity Advisory" states, *inter alia*, that:

a. "AvosLocker affiliates have compromised organizations across multiple critical infrastructure sectors in the United States[.]"[17]

b. "AvosLocker affiliates then use exfiltration-based data extortion tactics with threats of leaking and/or publishing stolen data."[18]

45. In fact, AvosLocker is especially notorious for ***publishing*** stolen PII. After all, an official white paper by the CISA revealed, *inter alia*, that:

a. "AvosLocker claims to directly handle ransom negotiations, as well as the publishing and hosting of exfiltrated victim data after their affiliates infect targets."[19]

b. "The leak site includes samples of stolen victim data and threatens to sell the data to unspecified third parties, if a victim does not pay the ransom."[20]

c. "The public leak site lists victims of AvosLocker, along with a sample of data allegedly stolen from the victim's network."[21]

---

[16] *California Northstate University student and employee data stolen*, DATABREACHES.NET (Feb. 15, 2023) https://databreaches.net/2023/02/15/california-northstate-university-student-and-employee-data-stolen/; *see also HACKS OF THE DAY 24/02/2023*, HACKMANAC, https://hackmanac.com/news/hacks-of-the-day-24-02-2023 (last visited June 10, 2024); *AvosLocker*, RANSOMLOOK, https://www.ransomlook.io/group/avoslocker, (last visited June 10, 2024).

[17] *Cybersecurity Advisory: AvosLocker*, CISA (Oct. 11, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a.

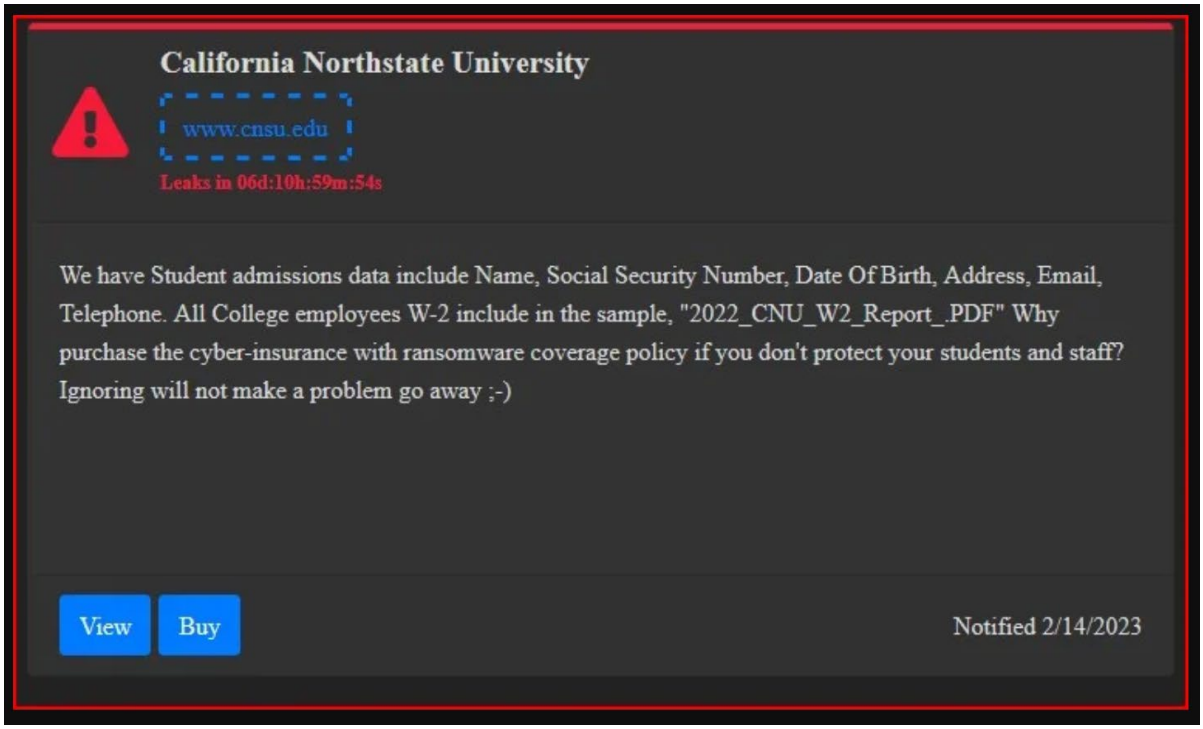
[18] *Id.*

[19] *Indicators of Compromise Associated with AvosLocker Ransomware*, CISA (March 17, 2022) https://www.ic3.gov/Media/News/2022/220318.pdf.

[20] *Id.*

[21] *Id.*

d. "The leak site gives visitors an opportunity to view a sample of victim data and to ***purchase victim data***."[22]



46. Here, AvosLocker has revealed that:

a. "We have Student admissions data include Name, Social Security Number, Date Of Birth, Address, Email, Telephone."[23]

b. "All College employees W-2 include in the sample, '2022_CNU_W2_Report_.PDF.'"[24]

47. Critically, AvosLocker has already ***published*** the stolen PII and has provided links for other cybercriminals to "View" and "Buy" that stolen PII.[25]

48. Thus, on information and belief, Plaintiffs' and Class Members' PII has already been published—or will be published imminently—on the Dark Web by cybercriminals like AvosLocker.

---

[22] *Id.* (emphasis added).
[23] *California Northstate University student and employee data stolen*, DATABREACHES.NET (Feb. 15, 2023) https://databreaches.net/2023/02/15/california-northstate-university-student-and-employee-data-stolen/.
[24] *Id.*
[25] *Id.*

C. Defendant was on Notice of the Foreseeable Risk of the Data Breach

49. In light of recent high profile data breaches, Defendant knew or should have known the electronic records and PII it maintained would be targeted by cybercriminals and ransomware attack groups.

50. Defendant knew or should have known that these attacks were common and foreseeable.

51. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[26] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[27]

52. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

D. Defendant Fails to Comply with FTC Guidelines.

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[28] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack

[26] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[27] *Id.*
[28] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 30, 2024).

the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. These FTC enforcement actions include actions against private universities like Defendant.

58. Defendant failed to properly implement basic data security practices.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

60. Defendant was at all times fully aware of its obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Fails to Comply with Industry Standards.

61. Several best practices have been identified that at a minimum should be implemented by companies storing sensitive PII like Defendant, including but not limited to: 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.

[29] *Id.*

62. Other best cybersecurity practices that are standard 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; training staff regarding critical points.

63. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

F. Defendant's Breach

65. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. failing to adequately protect PII;

c. failing to properly monitor their own data security systems for existing intrusions;

d. failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. failing to ensure the confidentiality and integrity of electronic PII it created,

received, maintained, and/or transmitted;

f. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

j. failing to train all members of their workforces effectively on the policies and procedures regarding PII;

k. failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTCA;

m. failing to adhere to industry standards for cybersecurity as discussed above; and,

n. otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

66. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access Defendant's computer systems, which provided unauthorized actors with unsecured and unencrypted PII.

67. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft.

68. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

69. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

70. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

71. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from

[30] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, U.S. GOV. ACCOUNTING OFFICE, (2007) https://www.gao.gov/new.items/d07737.pdf.

their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

72. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

73. Identity thieves can also use Social Security numbers 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 Social Security number, 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 being issued in the victim's name.

74. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[32]

75. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

76. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

77. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt

[31] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last accessed May 30, 2024).

[32] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

78. PII is such a valuable commodity to identity-thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

79. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

80. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

81. PII can sell for as much as $363 per record according to the Infosec Institute.[34] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

82. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[35] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[36] Each of these fraudulent activities is difficult to detect. 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.

83. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

84. An individual cannot obtain a new Social Security number without significant

---

[33] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, U.S. GOV. ACCOUNTING OFFICE, (2007) https://www.gao.gov/new.items/d07737.pdf.

[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[35] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 30, 2024).

[36] *Id* at 4.

paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[37]

85. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[38]

86. Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

H. Plaintiffs' and Class Members' Damages

87. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

88. Defendant has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to one year, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

89. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

90. Plaintiffs and Class Members' full names and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software maintaining PII. This PII was acquired by some unauthorized, unidentified third-party threat actor.

91. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the

[37] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[38] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

92. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis trying to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

93. Plaintiffs' PII was compromised as a direct and proximate result of the Data Breach.

94. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

95. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

96. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

97. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

98. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

99. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

100. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

101. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct

result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts; and

f. closely reviewing and monitoring Social Security numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

102. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

103. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

104. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Sankar's Experience

105. Plaintiff Sankar provided his information to Defendant as a condition of applying for admission to the institution.

106. Plaintiff Sankar provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

107. Plaintiff Sankar is very careful about sharing his sensitive private information. Plaintiff Sankar has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

108. Plaintiff Sankar first learned of the Data Breach after receiving a Notice of Breach on or about December 21, 2023, which advised that his PII was compromised in the Data Breach.

109. As a result of the Data Breach, Plaintiff Sankar made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

110. Plaintiff Sankar has spent significant time and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

111. Plaintiff Sankar suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Sankar; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

112. As a result of the Data Breach, Plaintiff Sankar has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Sankar is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

113. As a result of the Data Breach, Plaintiff Sankar anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Sankar will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

114. Plaintiff Sankar has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Titus-Lay's Experience

115. Plaintiff Titus-Lay was employed by Defendant from approximately 2017 to 2022. As a condition of her employment, Defendant required Plaintiff Titus-Lay to provide it with her PII, including but not limited to her full name and Social Security number.

116. Plaintiff Titus-Lay provided her PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

117. Plaintiff Titus-Lay's PII was compromised in the Data Breach.

118. Plaintiff Titus-Lay is very careful about sharing her sensitive private information. Plaintiff Titus-Lay has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

119. Defendant also deprived Plaintiff Titus-Lay of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it in a timely manner.

120. As a result of the Data Breach, Plaintiff Titus-Lay made reasonable efforts to mitigate the impact of the Data Breach including but not limited to monitoring her accounts and freezing her credit with the three major credit bureaus.

121. Plaintiff Titus-Lay has spent significant time and will continue to spend valuable hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

122. Plaintiff Titus-Lay suffered actual injury from having her PII compromised as a result

of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant maintained belonging to Plaintiff Titus-Lay; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

123. Indeed, following the Data Breach, Plaintiff Titus-Lay began experiencing a dramatic increase in scam and spam phone calls. For example, approximately 3–4 times per week, Plaintiff Titus-Lay receives targeted scam calls (which claim to be selling health insurance).

124. Critically, Plaintiff Titus-Lay has already suffered from identity theft and fraud:

a. her W2—which contains a treasure trove of highly sensitive PII—was published on the Dark Web by cybercriminals; and

b. cybercriminals fraudulently filed taxes under her name for the 2022 tax year.

125. Clearly, Plaintiff Titus-Lay's PII is in the hands of cybercriminals (who have stolen her identity and are actively committing fraud in her name).

126. As a result of the Data Breach, Plaintiff Titus-Lay has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Titus-Lay is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

127. As a result of the Data Breach, Plaintiff Titus-Lay anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff Titus-Lay will continue to be at a present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

128. Plaintiff Titus-Lay has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Cavanaugh's Experience

129. Plaintiff Cavanaugh was employed by Defendant from approximately 2020 until

2022. As a condition of his employment, Defendant required Plaintiff Cavanaugh to provide it with his PII, including but not limited to his full name and Social Security number.

130. Plaintiff Cavanaugh provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

131. Plaintiff Cavanaugh's PII was compromised in the Data Breach.

132. Plaintiff Cavanaugh is very careful about sharing his sensitive private information. Plaintiff Cavanaugh has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

133. Defendant also deprived Plaintiff Cavanaugh of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it in a timely manner.

134. As a result of the Data Breach, Plaintiff Cavanaugh made reasonable efforts to mitigate the impact of the Data Breach including but not limited to monitoring his accounts and putting a lock on his credit.

135. Plaintiff Cavanaugh has spent significant time and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

136. Plaintiff Cavanaugh suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Cavanaugh; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

137. Indeed, following the Data Breach, Plaintiff Cavanaugh began experiencing a dramatic increase in scam and spam text messages.

138. Critically, Plaintiff Cavanaugh has already suffered from identity theft and fraud:

a. cybercriminals fraudulently filed taxes under his name for the 2022 tax year.

139. Clearly, Plaintiff Cavanaugh's PII is in the hands of cybercriminals (who have stolen

his identity and are actively committing fraud in his name).

140. As a result of the Data Breach, Plaintiff Cavanaugh has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Cavanaugh is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

141. As a result of the Data Breach, Plaintiff Cavanaugh anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff Cavanaugh will continue to be at a present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

142. Plaintiff Cavanaugh has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Vongnalith's Experience

143. Plaintiff Vongnalith was employed by Defendant from approximately 2020 until 2023. As a condition of her employment, Defendant required Plaintiff Vongnalith to provide it with her PII, including but not limited to her full name and Social Security number.

144. Plaintiff Vongnalith provided her PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

145. Plaintiff Vongnalith's PII was compromised in the Data Breach.

146. Plaintiff Vongnalith is very careful about sharing her sensitive private information. Plaintiff Vongnalith has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

147. Defendant also deprived Plaintiff Vongnalith of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it in a timely manner.

148. Plaintiff Vongnalith has spent significant time and will continue to spend valuable

hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

149. As a result of the Data Breach, Plaintiff Vongnalith made reasonable efforts to mitigate the impact of the Data Breach. Thus far, she has spent over 40 hours:

a. calling the IRS regarding the fraudulent filing of her tax return;

b. consulting with CPAs;

c. filing a police report;

d. disputing a fraudulent credit inquiry; and

e. signing up for credit monitoring.

150. Notably, Plaintiff Vongnalith reached out to Defendant and asked for credit monitoring—but Defendant failed to respond and did not provide the credit monitoring promised.

151. Indeed, following the Data Breach, Plaintiff Vongnalith began experiencing a dramatic increase in scam and spam phone calls and texts.

152. Critically, Plaintiff Vongnalith has ***already*** suffered from identity theft and fraud:

a. cybercriminals fraudulently filed taxes under her name for the 2022 tax year (she was notified by TurboTax);

b. there was a fraudulent inquiry on her credit report in or around February 2023; and

c. her W2 and Social Security number were published on the Dark Web by cybercriminals (she was notified by Chase and TurboTax).

153. Clearly, Plaintiff Vongnalith's PII is in the hands of cybercriminals (who have stolen her identity and are actively committing fraud in her name).

154. Notably, the IRS told Plaintiff Vongnalith that Defendant should report the Data Breach to the IRS. Thereafter, Plaintiff Vongnalith urged Defendant to report the Data Breach in a timely manner. And upon information and belief, Defendant either failed to report the Data Breach to the IRS or failed to do so in a timely manner.

155. Plaintiff Vongnalith suffered actual injury from having her PII compromised as a

result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant maintained belonging to Plaintiff Vongnalith; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

156. As a result of the Data Breach, Plaintiff Vongnalith has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Vongnalith is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

157. As a result of the Data Breach, Plaintiff Vongnalith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff Vongnalith will continue to be at a present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

158. Plaintiff Vongnalith has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

159. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated under Federal Rule of Civil Procedure 23.

160. Plaintiffs propose the following Class and Sub-class definition (together, "Class"), subject to amendment as appropriate:

> National Class: All persons whose PII was compromised in the Data Breach, including all who were sent a Notice of Breach ("National Class").
>
> California Sub-class: All California citizens whose PII was compromised in the Breach, including all who were sent a Notice of Breach ("California Sub-class").

161. The California Sub-class is represented by Plaintiffs Titus-Lay, Cavanaugh, and Vongnalith (together, "California Plaintiffs").

162. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

163. Plaintiffs reserve the right to amend or modify the Class definitions as this case progresses.

164. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

165. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. if Defendant 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 Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendant owed a duty to Class Members to safeguard their PII;

f. if Defendant breached their duty to Class Members to safeguard their PII;

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiffs and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

166. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

167. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

168. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

169. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class

Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

170. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

171. Likewise, particular issues under Federal Rule of Civil Procedure 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. if Defendant failed to timely notify the public of the Data Breach;

b. if Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. if Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendant's failure to institute adequate protective security measures amounted to negligence;

e. if Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

172. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

173. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

174. Plaintiffs and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for admissions purposes only, and/or not disclose their PII to unauthorized third parties.

175. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

176. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

177. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

178. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

179. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

180. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

181. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

182. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. failing to adequately monitor the security of their networks and systems;

d. failing to have in place mitigation policies and procedures;

e. allowing unauthorized access to Class Members' PII;

f. failing to detect in a timely manner that Class Members' PII had been compromised; and

g. failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

183. Defendant owed to Plaintiffs and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

184. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant

to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

185. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

186. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and Class Members' PII.

187. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

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

189. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

190. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's 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.

191. Defendant's breach of its 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 PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data B reach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

192. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

193. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of receiving services and/or employment provided by Defendant. Plaintiffs and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's services and/or employment.

194. Plaintiffs and Class Members reasonably understood that a portion of the funds they paid Defendant (or funds derived from their employment) would be used to pay for adequate cybersecurity measures.

195. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that it was required to provide based on Defendant's duties under state and federal law and its internal policies.

196. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for services and/or employment.

197. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

198. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

199. After all, Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

200. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

201. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

202. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

203. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

204. In these and other ways, Defendant violated its duty of good faith and fair dealing.

205. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

206. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

207. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

208. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

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

210. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

211. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

212. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

213. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

214. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

215. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

216. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

217. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

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

219. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

220. Plaintiffs, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's 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.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

221. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

222. This count is pleaded in the alternative to breach of implied contract.

223. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiffs and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

224. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

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

226. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

227. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

228. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

229. Plaintiffs and Class Members have no adequate remedy at law.

230. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures as long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the impact of the PII comprised as a result of the Data Breach for the reminder of the lives of Plaintiffs and Class Members.

231. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

232. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

233. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

234. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

235. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

236. Because of the highly sensitive nature of the PII, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

237. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII.

238. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

239. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SIXTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
[Cal. Bus. & Prof. Code § 17200, et seq. – Unlawful Business Practices]
(On Behalf of Plaintiffs and the Class)

240. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

241. This count is brought by Plaintiffs on behalf of themselves and the putative Class.

242. Defendant violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

243. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods for safeguarding the PII of Plaintiffs and the Class Members.

244. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

245. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

246. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful

practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

247. Plaintiffs, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

SEVENTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff Titus-Lay and the California Sub-class)

248. Plaintiff Titus-Lay (for purposes of this cause of action, "Plaintiff") repeats and re-alleges paragraphs 1 through 172 of this Complaint and incorporates them by reference herein.

249. This count is brought by Plaintiff on behalf of herself and the putative California Sub-class.

250. Defendant 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 PII of Plaintiff and the California Sub-class. As a direct and proximate result, Plaintiff and the California Sub-class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

251. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is 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." Civil Code § 1798.140(d).

252. Plaintiff and California Sub-class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security

procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's and California Sub-class Members' PII. Plaintiff and California Sub-class Members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

253. On May 8, 2024, pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate.

254. Thereafter, Defendant failed to (1) respond to Plaintiff's CCPA notice letter, or (2) cure the alleged CCPA violations within the 30-day period allowed by § 1798.150(b).

255. Thus, Plaintiff and California Sub-class Members now seek statutory damages of "seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater" pursuant to § 1798.150(a)(1)(A).

256. As described herein, an actual controversy has arisen and now exists as to whether Defendant 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.

257. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

EIGHTH CAUSE OF ACTION
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of California Plaintiffs and the California Sub-class)

258. California Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

259. This count is brought by California Plaintiffs on behalf of themselves and the putative California Sub-class.

260. 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).

261. The Data Breach constitutes a "breach of the security system" of Defendant.

262. An unauthorized person acquired the personal, unencrypted information of California Plaintiffs and the California Sub-class.

263. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of California Plaintiffs and the California Sub-class but waited over ten months to notify them. Given the severity of the Data Breach, ten months was an unreasonable delay.

264. Defendant's unreasonable delay prevented California Plaintiffs and the California Sub-class from taking appropriate measures from protecting themselves against harm.

265. Because California Plaintiffs and California Sub-class Members were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

266. California Plaintiffs and California Sub-class Members are entitled to equitable relief and damages in an amount to be determined at trial.

NINTH CAUSE OF ACTION
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

267. Plaintiffs repeat and re-allege paragraphs 1 through 172 of this Complaint and incorporate them by reference herein.

268. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes

described above.

269. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

270. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTCA;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

271. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its prospective, current and/or former students' and employees' (i.e., Plaintiffs' and the Class') data.

272. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and

the Class, which include monetary damages that are not legally quantifiable or provable.

273. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

274. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order;

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the

privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training

program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to

evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: June 14, 2024

Respectfully Submitted,

By: */s/ Kristen Lake Cardoso*
Kristen Lake Cardoso (SBN 338762)
KOPELOWITZ OSTROW P.A.
One W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Tel: (954) 990-2218
cardoso@kolawyers.com

Scott Edelsberg (CA Bar No. 330990)
EDELSBERG LAW, P.A.
1925 Century Park E #1700
Los Angeles, CA 90067
Tel: (305) 975-3320
scott@edelsberglaw.com

Andrew G. Gunem (SBN 354042)
Cassandra Miller (*pro hac vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: (872) 263-1100
agunem@straussborrelli.com
cmiller@straussborrelli.com

Attorneys for Plaintiffs and the Proposed Class

ClassAction.org
