Andrew G. Gunem (SBN 354042)
Cassandra Miller (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
andrewg@turkestrauss.com
cassandram@turkestrauss.com

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

ERIKA TITUS-LAY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CALIFORNIA NORTHSTATE UNIVERSITY, LLC,

Defendant.

Case No. 2:24-at-00536

CLASS ACTION COMPLAINT

FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **NEGLIGENCE *PER SE*;**
3. **BREACH OF IMPLIED CONTRACT;**
4. **INVASION OF PRIVACY;**
5. **UNJUST ENRICHMENT;**
6. **BREACH OF FIDUCIARY DUTY;**
7. **CALIFORNIA UNFAIR COMPETITION LAW;**
8. **CALIFORNIA CONSUMER PRIVACY ACT;**
9. **CALIFORNIA CUSTOMER RECORDS ACT;**
10. **DECLARATORY JUDGMENT**

DEMAND FOR JURY TRIAL

Plaintiff Erika Titus-Lay ("Plaintiff") brings this Class Action Complaint, on behalf of herself and all others similarly situated (the "Class") against Defendant California Northstate University, LLC ("CNSU" or "Defendant") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach"). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current employees and current, former, and prospective students.

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of former and current employees' and former, current, and prospective students' highly personal information, including names, Social Security numbers, dates of birth, addresses, email addresses, telephone numbers, and W-2 forms ("personally identifying information" or "PII").[1]

3. On information and belief, the Data Breach occurred between February 12, 2023 and February 13, 2023, providing cybercriminals unfettered access to its network system until CNSU discovered the Breach.

4. CNSU struggled to identify what information and which individuals were impacted by the Data Breach and took until November 2, 2023, to complete its internal investigation.

5. On December 21, 2023, CNSU finally began notifying Class Members about the Data Breach ("Notice Letter").

6. CNSU waited more than ten months before finally informing Class Members of the Breach, even though Plaintiff and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss

[1] https://databreaches.net/california-northstate-university-student-and-employee-data-stolen/, (last visited April 22, 2024).

of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

7. CNSU's Breach Notice also obfuscated the nature of the breach and the threat it posted—refusing to tell its former and current employees and students how many people were impacted, how the breach happened, or why CNSU delayed notifying victims that hackers had gained access to highly sensitive PII.

8. Defendant's failure to timely detect and report the Data Breach made its employees and students vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its employees.

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff is a former employee of CNSU and is a Data Breach victim. Plaintiff worked for CNSU from 2017-2022.

13. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

14. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, employees' private information was exactly that—private. Not anymore. Now, employees' and students' private information is forever exposed and unsecure.

PARTIES

15. Plaintiff, Erika Titus-Lay, is a natural person and citizen of California, where she intends to remain. Plaintiff is a Data Breach victim.

16. Defendant, California Northstate University, LLC is a corporation formed in Delaware and registered in good standing in California. CNSU's principal place of business is 9700 West Tarib Drive, Elk Grove, CA 95757.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the proposed Class is a citizen of a state different from that of CNSU.

18. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

California Northstate University

20. CNSU is a private university specializing in healthcare education. CNSU consists of seven colleges and offers 15 professional and undergraduate programs. CNSU employs over 200 individuals and has over 1,500 graduates.[2] CNSU boasts an annual revenue of $69.5 million.[3]

[2] https://www.cnsu.edu/ (last visited April 22, 2024).
[3] https://www.zoominfo.com/c/california-northstate-university/348774309 (last visited April 22, 2024).

21. On information and belief, CNSU accumulates highly sensitive PII of its current and former employees and students.

22. On information and belief, CNSU maintains current and former employees' and students' PII for years—even decades—after their relationship is terminated.

23. In collecting and maintaining its employees' and students' PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

24. Indeed, CNSU assures its students that "[t]he university does not disclose social security numbers, student or personal identification numbers…"[4]

25. Further, CNSU's Online Privacy Policy states that Defendant takes "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."[5]

26. In collecting and maintaining employees' and students' PII, CNSU agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

27. Despite recognizing its duty to do so, on information and belief, CNSU has not implemented reasonably cybersecurity safeguards or policies to protect its former and current employees' and students' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, CNSU leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

The Data Breach

28. Plaintiff is a former employee of CNSU.

[4]https://www.cnsu.edu/registrar/ferpa.php#:~:text=The%20university%20does%20not%20disclose,has%20signed%20a%20consent%20form (last visited April 22, 2024).

[5] https://www.cnsu.edu/privacy/ (last visited April 22, 2024).

29. As a condition of employment with and/or receiving educational services from CNSU, employees and students were required to disclose their PII to Defendant, including but not limited to, their names and Social Security numbers. Defendant used that PII to facilitate employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

30. On information and belief, CNSU collects and maintains former and current employees' and students' unencrypted PII in its computer systems.

31. In collecting and maintaining the PII, CNSU implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

32. According to the Breach Notice, CNSU "recently completed its investigation of an incident that involved unauthorized access to certain University computer systems." Following its internal investigation, CNSU discovered that "between February 12, 2023 and February 13, 2023, an unauthorized actor potentially accessed and obtained certain files stored on our servers." Ex. A.

33. In other words, CNSU's investigation revealed that Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its former and current employees' and students' highly sensitive PII.

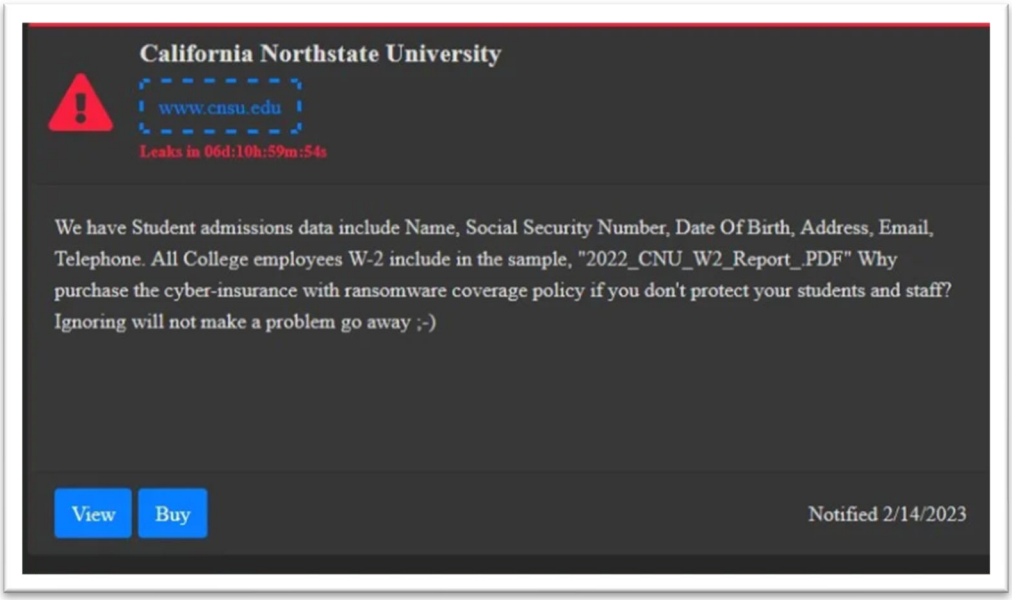
34. Additionally, Defendant admitted that Plaintiff's and the Class's PII were actually stolen during the Data Breach, confessing that victims' information was not just accessed but that the cybercriminals "obtained certain files" from Defendant's network. Ex. A.

35. Upon information and belief, the AvosLocker ransomware group was responsible for the cyberattack. AvosLocker is a "ransomware variant that sports the staples of modern ransomware" and is "slowly making a name for itself, with the [FBI] releasing an advisory on

[AvosLocker]" in March 2022.[6] Defendant knew or should have known of the tactics that groups like AvosLocker employ.

36. With the Sensitive Information secured and stolen by AvosLocker, the hackers then purportedly issued a ransom demand to CNSU. However, CNSU has provided no public information on the ransom demand or payment.

37. On February 14, 2023, AvosLocker released a statement regarding the types of information it obtained from the Breach on a data leak page. On information and belief, AvosLocker posted the 2022 W-2 statements for the CNSU's President and CEO, Vice-President, CFO, and an applicant's information.[7]



38. On or around December 21, 2023, –more than ten months after the Breach first occurred– CNSU finally began notifying Class Members about the Data Breach.

39. Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

[6] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker (last visited April 22, 2024).
[7] https://databreaches.net/california-northstate-university-student-and-employee-data-stolen/ (last visited April 22, 2024).

40. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing employees' and students' PII, as evidenced by the Data Breach.

41. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

42. In response to the Data Breach, Defendant contends that it has "implemented additional security measures to enhance the security of its network." Ex. A. Although Defendant does not elaborate on what these "enhancements" are, such enhancements should have been in place before the Data Breach.

43. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." Ex. A.

44. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

45. On information and belief, CNSU has offered twelve months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

46. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

47. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement

reasonable security measures, causing it to lose control over its employees' and students PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

48. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the academic/education industries preceding the date of the breach.[8]

49. In light of recent high profile data breaches at other academic institutions, Defendant knew or should have known that its employees' PII would be targeted by cybercriminals.

50. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9] 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.[10]

51. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [11]

---

[8] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited August 3, 2023); *See also* Cost of a Data Breach: Infrastructure, security Intellegancehttps://securityintelligence.com/articles/cost-data-breach-infrastructure/ (last visited April 22, 2024).

[9] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited April 22, 2024).

[10] *Id*.

[11] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited April 22, 2024).

52. In 2023, manufacturing and infrastructure adjacent industries were warned to be one of the most-breached sectors[12] and cost, on average, $4.82 million per breach.[13]

53. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report cautioned, "Cyber risk in the financial system has grown over time as the system has become more digitized, as evidenced by the increase in cyber incidents."[14]

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

Plaintiff's Experience

55. From approximately 2017 until 2022 Plaintiff Titus-Lay was employed by Defendant.

56. As a condition of employment, CNSU required Plaintiff to provide her PII, including but not limited to her full name and Social Security number.

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

58. Plaintiff's PII, including at least her full name and Social Security number, may have been compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Plaintiff to be at substantial risk for further identity theft.

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

---

[12] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited April 22, 2024).

[13] Cost of a Data Breach: Infrastructure, security Intellegancehttps://securityintelligence.com/articles/cost-data-breach-infrastructure/ (last visited April 22, 2024).

[14] Implications of Cyber Risk for Financial Stability, Federal Reserve, https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited April 22, 2024).

60. Plaintiff suffered actual injury from the exposure of her PII —which violates her rights to privacy.

61. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

62. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

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

64. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

65. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

66. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

67. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

68. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, including, time spent:

a. monitoring her accounts; and

b. freezing her credit with the three major credit bureaus.

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

70. Critically, Plaintiff 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.

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

72. Plaintiff 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 and the Proposed Class Face Significant Risk of Continued Identity Theft

73. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

74. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

75. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

76. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

77. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

78. One such example of criminals using PII for profit is the development of "Fullz" packages.

79. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

80. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be

included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

81. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity including theft and sale on the dark web. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

82. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

83. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

84. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

85. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

86. The FTC recommends that companies not maintain information 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.

87. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

88. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers, or in this case former and current employees', PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

89. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. Several best practices have been identified that a minimum should be implemented by employers in possession of 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.

Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard for employers 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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

92. 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.

93. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

94. Plaintiff sues on behalf of herself and the proposed class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose PII was compromised in the California Northstate University Data Breach including all those who received notice of the breach.

95. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's

officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

96. Plaintiff reserves the right to amend the class definition.

97. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The exact number of Class members is unknown but is estimated to be up to thousands of former and current CNSU employees and students at this time, and individual joinder in this case is impracticable.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control.

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether 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;

iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

98. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

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

99. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

101. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

102. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

103. Defendant owed these duties to Plaintiff 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 practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII.

104. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII.

105. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff 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.

106. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

107. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

108. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

109. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold 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.

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

111. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

112. Defendant breached these duties as evidenced by the Data Breach.

113. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

114. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

115. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

116. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

117. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

119. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff 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 Breach 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
Negligence *per se*
(On Behalf of Plaintiff and the Class)

120. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

121. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

122. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII.

123. Defendant breached its respective duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

124. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

125. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

126. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class members would not have been injured.

127. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

128. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

129. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

130. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

131. Plaintiff and Class members were required to provide their PII to Defendant as a condition of receiving services and/or employment provided by Defendant. Plaintiff and Class

members provided their PII to Defendant or its third-party agents in exchange for Defendant's services and/or employment.

132. Plaintiff 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.

133. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

134. Plaintiff 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.

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

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

137. After all, Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

138. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

139. 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.

140. 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.

141. Defendant materially breached the contracts it entered with Plaintiff 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.

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

143. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

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

145. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

147. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

148. Defendant owed a duty to its employes and students, including Plaintiff and the Class, to keep this information confidential.

149. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII is highly offensive to a reasonable person.

150. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

151. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

152. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

153. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

154. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

155. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

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

157. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

158. Plaintiff and the Class 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 Plaintiff and the Class.

159. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class members, also 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.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

160. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

162. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide services and/or facilitate employment.

163. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

164. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

165. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

166. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures.

Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

167. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' employment, payment, and/or PII because Defendant failed to adequately protect their PII.

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

169. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

170. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

171. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff 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.

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

173. Because of the highly sensitive nature of the PII, Plaintiff 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.

174. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

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

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

SEVENTH CAUSE OF ACTION
Violation of California's Unfair Competition Law (UCL)
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff and the Class)

177. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

178. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

179. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*. (the "CRA"), and other state data security laws.

180. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure to prevent the loss or misuse of that PII.

181. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

182. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

183. Had Defendant complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

184. Defendant's conduct was unlawful, in that it violated the CCPA.

185. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

186. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

187. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

188. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

189. Instead, Defendant made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

190. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

191. For one, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the dark web.

192. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

193. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

194. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

EIGHTH CAUSE OF ACTION
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the Class)

195. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

196. 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 Class. As a direct and proximate result, Plaintiff's and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

197. 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).

198. Plaintiff and 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 Class members' PII. Plaintiff and 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.

199. 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. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

200. 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.

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

NINTH CAUSE OF ACTION
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff and the Class)

202. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

203. 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).

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

205. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

206. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class but waited over ten months to notify them. Given the severity of the Data Breach, ten months was an unreasonable delay.

207. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

208. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

209. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

TENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

210. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

211. 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. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

212. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

213. Given 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 use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

214. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

215. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

216. And if a second breach occurs, Plaintiff and the Class will lack 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 for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

217. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

218. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the putative Class, demands a trial by jury on all claims so triable.

Dated: April 29, 2024

By: */s/ Andrew G. Gunem*

Andrew G. Gunem (SBN 354042)
Cassandra Miller (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
andrewg@turkestrauss.com
cassandram@turkestrauss.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org