LINDEMANN LAW FIRM, APC
BLAKE J. LINDEMANN, SBN 255747
DONNA R. DISHBAK, SBN 259311
9777 Wilshire Blvd., 4th Floor
Beverly Hills, CA 90212
Telephone: (310) 279-5269
Facsimile: (310) 300-0267
E-Mail: blake@lawbl.com

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

HELEN JIA, on behalf of herself and all others similarly situated,

Plaintiffs,

vs.

WEEE! INC.,

Defendant.

Case No.

COMPLAINT FOR DAMAGES FOR:

1. **Intrusion Upon Seclusion**
2. **California Constitutional Right to Privacy**
3. **Violation of The California Unfair Competition Law**
4. **Violation of The California Customer Records Act**
5. **Violation of The California Information Practices Act**
6. **Breach of Confidentiality**
7. **Constructive Fraud**
8. **Breach of Express Contract**
9. **Breach of Implied Contract**
10. **Unjust Enrichment**
11. **Declaratory Relief**
12. **Negligence/Gross Negligence/Negligence Per Se**
13. **California Consumer Privacy Act**

[Demand for Jury Trial]

Plaintiff Helen Jia, on her own behalf and those similarly situated ("Plaintiffs"), hereby file this complaint against Weee!, Inc., and DOES 1-100 (collectively, the "Defendants"), and demanding a trial by jury, aver as follows:

INTRODUCTION

1. This case concerns a February 2023 data breach event by one of the largest national grocers for Asian American, Weee!, and specifically targets Chinese immigrants like Plaintiff and representative Helen Jia.

JURISDICTION AND VENUE

2. This Court has personal jurisdiction over the Defendants as they regularly transact business in this judicial district, and in fact this Case is filed in the District of Defendant Weee!'s principal place of business at 47467 Fremont Blvd., Fremont, CA 94538. Pursuant to L.R. 3-2(c), the address giving rise to the Case is in Alameda County, which is assigned "San Francisco and Oakland."

3. Venue is proper in this judicial district because a substantial part of the events giving rise to the causes of action occurred in this district.

THE PARTIES

4. Plaintiff Helen Jia is a citizen and resident of the County of Orange, California.

5. Defendant WEEE! Inc. is a corporation with its principal place of business at 47467 Fremont Blvd., Fremont, CA 94538.

6. Plaintiffs are ignorant of the true names and capacities of the Defendants DOES 1 through 100, inclusive, whether individual, corporate, associate, or otherwise, and therefore have sued them by the foregoing names which are fictitious. Plaintiffs ask that when their true names and capacities are discovered that this Complaint may be amended by inserting their true names and capacities in lieu of said fictitious names, together with apt and proper words to charge them. All references to any named Defendants shall also refer to said Does. When the true names and capacities are ascertained, Plaintiffs will amend this Complaint accordingly. On information and belief, Plaintiffs allege that each of the fictitiously named defendants was responsible in some manner for the acts and omissions alleged herein and are liable to Plaintiffs herein.

7. Said DOE defendants may include, but do not necessarily include, individuals, businesses, corporations, partnerships, associations, joint ventures, defendants that are government in nature, as well as product manufacturers, professionals, contractors, estates, administrators of estates, trusts and/or all other types of entities and/or individuals as discovery in the matter may reveal. Regardless, Plaintiffs allege that each of the defendants designated herein as DOE is legally responsible in some manner for the events and happenings herein referred to, and legally caused injury and damages proximately thereby to Plaintiffs and each of them are alleged.

8. Plaintiffs are informed and believe, and based thereon allege, that each of the defendants are the agent and/or employee of each and every other defendant, and in doing the things herein alleged, each defendant was acting in the course and scope of said agency and/or employment and that each of the acts of the defendants was ratified and confirmed by each and every other defendant.

9. Plaintiffs are informed and believe, and based thereon allege, that each of the defendants designated as a DOE is in some manner responsible for the events and happenings herein referred to, and caused injury and damages proximately thereby to Plaintiffs as herein alleged.

FACTS COMMON TO ALL CAUSES OF ACTION

10. Plaintiffs, individually and on behalf of all other similarly situated persons (the "Class Members"), bring this consumer class action to secure redress for Defendants' violations of their property and privacy rights. Plaintiff and Class Members are consumers who entrusted their personally identifiable information ("PII") to Defendants. Defendants betrayed Plaintiffs and Class Members' trust by failing to properly safeguard and protect their PII, and publicly disclosing their PII without authorization, in violation of numerous laws, including, *inter alia*, the California Customer Records Act ("CRA") (Cal. Civ. Code § 1798.80, *et seq*.), California Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code § 17200, *et seq*.), California Information Practices Act ("IPA") (Cal. Civ. Code § 1798, *et seq*.), and California common law.

11. On February 6, 2023, a threat actor named "IntelBroker" began leaking the data of Weee!'s customers on the "Breached" hacking and data breach forum (the "Breach").

12. Reportedly, the Breach contained 1.1 million of Weee!'s customers who placed orders after July 12, 2021: first and last names, email addresses, phone numbers, device types (i.e., iOS, PC, or Android), order notes, and other data used by Weee!. Plaintiff Jia placed several orders after July 12, 2021.

13. Defendants' security failures enabled the hackers to steal personal and financial data from Defendant and put Class members' personal and financial information at serious and ongoing risk. The hackers continue to use the information they obtained as a result of Defendant's inadequate security to exploit and injure Class members across the United States.

14. The Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. Defendant grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Breach.

15. Defendant failed to uncover and disclose the extent of the Breach and notify its affected customers of the Breach in a timely manner. Defendant failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Breach. Furthermore, by failing to provide adequate notice, Defendant prevented Class Members from protecting themselves from the Breach.

16. Plaintiffs and Class Members are concerned about their finances, credit, identities, and PII and, as such, as to Helen Jia, regularly monitors her credit, monitor her financial accounts and/or carefully store and dispose of their PII and other documents containing their PII. The concern is reasonable and justified. Because of the Data Breach, there is an immediate and substantial risk of identity theft, identity fraud, and records, fraudulent credit card activity, the opening or re-opening of new credit card accounts in their name, phishing, increased mailers marketing products and services. Plaintiff has standing to bring this suit because as a direct and proximate result of Defendants' wrongful actions, inaction and omissions, and the resulting Data Breach, Plaintiffs have suffered (and will continue to suffer) economic damages and other injury and harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud - risks justifying

expenditures for protective and remedial services for which she is entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII, (iv) statutory damages under the California CMIA, (v) deprivation of the value of her PII, for which there is a well-established national and international market, and (vi) the financial and temporal cost of monitoring Helen Jia's credit, monitoring her financial accounts, and those of her children, and mitigating her damages.

The Data Breach

17. Defendants are responsible for allowing the Data Breach to occur because they failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in privacy statements and their explicit and implied agreements with customers.

18. During the duration of the Data Breach, Defendants failed to detect the unauthorized third parties' access to Defendants' systems and databases, notice the massive amounts of data that were compromised, and failed to take any steps to investigate the red flags that should have warned Defendants that their systems were not secure. As a result of Defendants' failure to protect the sensitive PII it was entrusted with, Plaintiffs and class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiffs and class members have also lost the inherent value of their PII.

19. Plaintiffs and class members provided their PII to Defendants and any necessary party working with Defendants, with the expectation and understanding that Defendants would adequately protect and store their data. If Plaintiffs and class members had known that Defendants' data security was insufficient to protect their PII, they would have demanded that Defendants not store their PII on Defendants' databases or process it through Defendants' systems.

Defendants Failed to Comply with Regulatory Guidance and Meet Consumers' Expectations

20. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

21. 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. Among other things, the guidelines note 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 their network's vulnerabilities; and implement policies to correct security problems. 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 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.

22. Additionally, the FTC recommends that companies 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.

23. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

24. In this case, Defendants were fully aware of their obligation to use reasonable measures to protect the PII of their customers, acknowledging as much in its own privacy policies. Defendants also knew that the Defendants' databases are the target for hackers. But despite understanding the consequences of inadequate data security, the Defendants failed to comply with industry standard data security requirements.

25. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 and various state consumer protection and data breach statutes.

Effect of the Data Breach

26. Defendants' failure to keep Plaintiffs' and class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach, cyber criminals have the ability to commit identity theft and other identity-related fraud against Plaintiffs and class members now and into the indefinite future.

27. The information stolen from Defendants included usernames and passwords-PII that is highly valued among cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for $15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay ($12), Amazon (≤$10), and Walmart (≤$10) fetch similar amounts. Consumers often reuse passwords. By unlawfully obtaining this information, cyber criminals can use these credentials to access other services beyond that which was hacked.

28. PII also has significant monetary value in part because criminals continue their efforts to obtain this data. In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred.

29. The value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

30. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.

31. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.

32. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of

PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

33. Even before the occurrence of identity theft, victims may spend valuable time and suffer from the emotional toll of a data breach. Here, Plaintiff Jia has already spent approximately four hours investigating the Data Breach after receiving notice from Defendants, including independent online research regarding the scope of the breach. She will continue to expend time monitoring his family's credit and other identity-related information and is exploring options for identity theft protection services because Defendants did not offer such services as a result of the Data Breach.

34. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages. For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

35. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively
    - impacted by the identity theft; and
- 7% reported feeling suicidal.

36. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.

37. There may also be a significant time lag between when PII is stolen and when it is actually misused. 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 to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

38. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII that was compromised in the Data Breach.

39. As the result of the Data Breach, Plaintiffs and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. identity theft and fraud resulting from theft of their PII;
b. costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;
c. losing the inherent value of their PII;
d. losing the value of Defendants' explicit and implicit promises of adequate data security;
e. costs associated with purchasing credit monitoring and identity theft protection services;

f. unauthorized access to and misuse of their online accounts;

g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, updating login information for online accounts sharing the same login credentials as were compromised in the Data Breach, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

j. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and

k. continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs and class members.

40. Additionally, Plaintiffs and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a

provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.

41. The cost of hosting or processing customers' PII on or through Defendants' databases and systems includes things such as the actual cost of the servers and employee hours needed to process said transactions. One component of the cost of using these services is the explicit and implicit promises Defendants made to protect customers' PII. Because of the value customers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if customers did not value their data security and privacy, companies like Defendants would have no reason to tout their data security efforts to their actual and potential customers.

42. Had the victims of the Data Breach including Plaintiffs known the truth about Defendants' data security practices—that Defendants would not adequately protect and store their data—they would have demanded that Defendants not store their PII on Defendants' databases or process it through Defendants' systems.

43. Plaintiffs and class members are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and Defendants' deceptive and unconscionable conduct.

CLASS ACTION ALLEGATIONS

44. Pursuant to Fed. R. Civ. Proc. 23, Plaintiffs seek certification on behalf of two subclasses, defined as follows:

45. **National Class**: All customers in the United States whose PII was compromised in the Data Breach.

46. **California Subclass**: All customers in California whose PII was compromised in the Data Breach.

47. The National Class, and California subclass are collectively referred to herein as the "Class."

48. Excluded from the Class are Defendants themselves, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors,

subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

49. **Risk of Inconsistent or Varying Adjudications**. As the proposed class members include tens, if not hundreds, of thousands of customers, there is significant risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Defendants. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

50. **Numerosity**. The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiffs at this time, Defendants has admitted that several databases in Defendants' hosting were compromised in the Data Breach, suggesting that thousands of customers were affected by the Data Breach.

51. **Commonality and Predominance**. This action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include, but are not limited to:

a. Whether Defendants knew or should have known that its computer and data storage systems were vulnerable to attack;

b. Whether Defendants omitted or misrepresented material facts regarding the security of its computer and data storage systems and their inability to protect vast amounts of sensitive data, including Plaintiffs' and class members' PII;

c. Whether Defendants failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

d. Whether Defendants failed to take available steps to prevent and stop the Data Breach from happening;

e. Whether Defendants failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard PII;

f. Whether Defendants owed duties to Plaintiffs and class members to protect their PII;

g. Whether Defendants owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

h. Whether Defendants breached their duties to protect the PII of Plaintiffs and class members by failing to provide adequate data security;

i. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and class members;

j. Whether Defendants' failure to secure Plaintiffs' and class members' PII in the manner alleged violated federal, state and local laws, or industry standards;

k. Whether Defendants was negligent, reckless or intentionally indifferent in its representations to Plaintiffs and class members concerning its security protocols;

l. Whether Defendants' conduct and practices described herein amount to acts of intrusion upon seclusion;

m. Whether Defendants was negligent in making misrepresentations to Plaintiffs and class members;

n. Whether Defendants was negligent in establishing, implementing, and following security protocols;

o. Whether the Plaintiffs' and class members' PII was compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

p. Whether Defendants' conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and class members' PII;

q. Whether Defendants has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

r. Whether Plaintiffs and class members were the intended third-party beneficiaries of any contractual obligations owed by Defendants;

s. Whether Defendants' conduct amounted to violations of California consumer protection and data breach statutes;

t. Whether, as a result of Defendants' conduct, Plaintiffs and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

u. Whether, as a result of Defendants' conduct, Plaintiffs and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief;

v. Whether Plaintiffs and class members are entitled to compensatory damages;

w. Whether the Plaintiffs and class members are entitled to punitive damages; and

x. Whether the Plaintiffs and class members are entitled to statutory damages.

52. **Typicality**. Plaintiffs' claims are typical of other class members' claims because Plaintiffs and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

53. **Adequacy**. Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class. All Plaintiffs are members of the Nationwide Class and the California Subclass, and Plaintiff Jia is a member of both sub-classes. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in privacy litigation and consumer protection claims. Plaintiffs intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

54. **Superiority**. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful

conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

55. **Injunctive and Declaratory Relief**. Class certification is also appropriate as an injunctive relief measure. Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendants continues to maintain their inadequate security practices, retains possession of Plaintiffs' and the class members' PII, and have not been forced to change their practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Intrusion Upon Seclusion

(Brought on Behalf of Plaintiffs and the Classes)

56. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

57. California adheres to Restatement (Second) of Torts, § 652B with no material variation.

58. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts, § 652B.

59. Defendants intentionally intruded on and into Plaintiffs' and Class members' solitude, seclusion, or private affairs by constructing an inadequate system to store data of customers.

60. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the data breach and tracking of children, centuries of common law, state and federal statutes and regulations, legislative

commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity.

61. Defendants' exploitation of immigrants' information through lax data and cybersecurity practices contributes to the highly offensive nature of Defendants' activities.

62. Plaintiffs and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

63. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class members.

64. As a result of Defendants' actions, Plaintiffs and Class members seek injunctive relief, in the form of Defendants' cessation of tracking practices in violation of state law, and destruction of all personal data obtained in violation of state law.

65. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

66. Plaintiffs seek restitution for the unjust enrichment obtained by Defendants' as a result of the Data Breach.

SECOND CAUSE OF ACTION

California Constitutional Right to Privacy

(Brought on Behalf of Plaintiffs and the Classes)

67. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

68. The California Supreme Court held in *Butt v. California* (1992) 4 Cal. 4th 668, 680, "California has assumed specific responsibility for a statewide public education system open on equal

terms to all." Specifically, the California Constitution guarantees both the right to privacy and the right to an education:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."
>
> "A general diffusion of knowledge and intelligence being essential to the preservation of the rights and liberties of the people, the Legislature shall encourage by all suitable means the promotion of intellectual, scientific, moral, and agricultural improvement."

69. Plaintiff Helen Jia in her own capacity, and Class members have reasonable expectations of privacy in their files with the Defendants.

70. The reasonableness of such expectations of privacy is supported by Defendants' unique position to monitor Plaintiffs' and Subclass members' as customers who are immigrants.

71. Defendants recklessly intruded on and into Plaintiffs' and Subclass members' solitude, seclusion, right of privacy, or private affairs by intentionally designing the computer systems and databases in a manner subject to, and vulnerable to a cybersecurity attack.

72. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential information about children, constituting an egregious breach of social norms. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Subclass members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity.

73. Plaintiffs and Subclass members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

74. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Subclass members.

75. As a result of Defendants' actions, Plaintiffs and Subclass members seek injunctive relief, in the form of Defendants' cessation of tracking practices in violation of state law, and destruction of all personal data obtained in violation of state law. As a result of Defendants' actions, Plaintiffs and Subclass members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions - which were malicious, oppressive, willful - were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

THIRD CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

(Cal. Bus. & Prof. Code § 17200, *et seq*.)

(On Behalf of Plaintiff and Each Class Member)

76. Plaintiffs re-allege and incorporate by reference herein each and every allegation contained herein above as though fully set forth and brought in this cause of action.

77. The California Unfair Competition Law, Cal Bus. & Prof. Code § 17200, *et seq*., prohibits any "unlawful, fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of their above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

78. In the course of conducting its business. Defendants committed "unlawful business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs and Class Members' PII, and violating the statutory and common law alleged herein in the process, including, *inter alia*, the California CMIA, the California CRA, and the California IPA. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business

acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

79. Defendants also violated the UCL by failing to timely notify Plaintiffs and Class Members regarding the unauthorized release (and/or threats of unauthorized release) and disclosure of their PII. If Plaintiffs and Class Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

80. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair business acts and practices" in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

81. The UCL also prohibits any "fraudulent business act or practice." Defendants' above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

82. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, risks justifying expenditures for protective and remedial identity fraud for which she is entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII, (iv) statutory damages under the California CMIA, (v) deprivation of the value of her PII, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring her credit, monitoring her financial accounts, and mitigating her damages.

83. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of

themselves and Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to them, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203.

FOURTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT

(Cal. Civ. Code § 1798.80, *et seq*.)

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

84. Plaintiffs re-allege and incorporate by reference herein each and every allegation contained herein above as though fully set forth and brought in this cause of action.

85. To ensure that personal information about California residents is protected, the California Legislature enacted the Customer Records Act, California Civil Code § 1798.81.5, which requires that any business that "owns licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

86. As described above. Defendants failed to implement and maintain reasonable security procedures and practices to protect the Plaintiffs and Class Members' PII, and thereby violated the California Customer Records Act.

87. Under California Civil Code § 1798.82, any business that obtains and retains PII must promptly and "in the most expedient time possible and without unreasonable delay" disclose any Data Breach involving such retained data.

88. By its above-described wrongful actions, inaction, omissions, and want of ordinary care. Defendants failed to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs and Class Members' PII.

89. Defendants also unreasonably delayed and failed to disclose the Data Breach (and threat of the data breach) to Plaintiffs and Class Members in the most expedient time possible and without unreasonable delay when they knew, or reasonably believed, Plaintiffs and Class Members' PII had been wrongfully disclosed to an unauthorized person or persons.

90. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the California CRA, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud - risks Justifying expenditures for protective and remedial services for which she is entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII, (iv) statutory damages under the California CMIA, (v) deprivation of the value of her PII, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring her credit, monitoring her financial accounts, and mitigating her damages.

91. Plaintiff is also entitled to injunctive relief under California Civil Code Section 1798.84(e).

FIFTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA INFORMATION PRACTICES ACT

(Cal. Civ. Code §§ 1798, *et seq*.)

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

92. Plaintiffs re-allege and incorporate by reference herein each and every allegation contained herein above as though fully set forth and brought in this cause of action.

93. Pursuant to the California Information Practices Act of 1977, California Civil Code § 1798.21, a company is required "to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury."

94. As described above, Defendants failed to implement and maintain reasonable security procedures and practices to protect the Plaintiffs and Class Members' PII, and thereby violated the California IPA.

95. Under California Civil Code § 1798.29, any agency that obtains and retains PII must promptly and "in the most expedient time possible and without unreasonable delay" disclose any Data Breach involving such retained data.

96. By its above-described wrongful actions, inaction, omissions, and want of ordinary care. Defendants failed to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs and Class Members PII.

97. Defendants also unreasonably delayed and failed to disclose the Data Breach to Plaintiffs and Class Members in the most expedient time possible and without unreasonable delay when they knew, or reasonably believed. Plaintiffs and Class Members' PII had been wrongfully disclosed to an unauthorized person or persons.

SIXTH CAUSE OF ACTION

BREACH OF CONFIDENTIALITY

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

98. Plaintiffs re-allege and incorporate by reference herein each and every allegation contained herein above as though fully set forth and brought in this cause of action.

99. Plaintiffs and Class Members' unique, personal, and private PII in Defendants' possession, custody, and control was (and continues to be) highly confidential.

100. Defendants breached the confidentiality of Plaintiff's and Class Members' PII by failing to identify, implement, maintain and monitor appropriate data security measures, policies, procedures, protocols, and/ software and hardware systems to ensure the security and confidentiality of Plaintiffs and Class Members' PII, and wrongfully releasing and disclosing their PII without authorization, as described above.

101. Had Defendants not engaged in the above-described wrongful actions, inaction and omissions, the Data Breach never would have occurred and Plaintiffs and Class Members' PII would

not have been wrongfully released, disclosed, compromised, disseminated to the world, and wrongfully used. Defendants' wrongful conduct constitutes (and continues to constitute) the tort of breach of confidentiality at California common law.

102. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud - risks justifying expenditures for protective and remedial services for which she is entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII, (iv) statutory damages under the California CMIA, (v) deprivation of the value of her PII, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring her credit, monitoring her financial accounts, and mitigating her damages.

SEVENTH CAUSE OF ACTION

CONSTRUCTIVE FRAUD

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

103. The preceding factual statements and allegations are incorporated by reference.

104. Defendants, in collecting Plaintiffs and Class Members' nonpublic, personal, financial, were therefore entrusted with Plaintiffs and Class Members' nonpublic personal, and financial information, and were put in the same confidential and special relationship with Plaintiffs and Class Members as they had with the companies that provided them with financial insurance.

105. Defendants breached their confidential and special relationship with Plaintiffs and Class Members by failing to adequately secure Plaintiffs and Class Members' nonpublic personal and financial information from unauthorized users, including cyber thieves who stole the information as described herein.

106. As a direct and proximate result of Defendants' breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

EIGHTH CAUSE OF ACTION

BREACH OF EXPRESS CONTRACT

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

107. The preceding factual statements and allegations are incorporated by reference.

108. Plaintiffs and Class Members, upon information and belief entered into express contracts with Defendants that include Defendants' promise to protect nonpublic personal information given to Defendants or that Defendants gather on their own, from disclosure. Defendants' promise was incorporated into each of the privacy policies, student manuals, and other enrollment documents issued to Plaintiffs and Class Members.

109. Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was accessed by unauthorized personnel as part of the cyber hacking Incident that occurred in 2023.

110. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

NINTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

111. Defendants provided Plaintiffs and Class Members with an implied contract to protect and keep Plaintiffs' private nonpublic personal, educational, and financial information when they gathered the information from each of their customers.

112. Plaintiffs and Class Members would not have provided their personal or financial and health information to Defendants or their subsidiaries, but for Defendants' implied promises to safeguard and protect Defendants' customers' nonpublic personal and financial information.

113. Plaintiffs and Class Members performed their obligations under the implied contract when they provided their private personal, educational, and financial information as customers and were furnished with the services provided by Defendants.

114. Defendants breached the implied contracts with Plaintiffs and Class Members by failing to protect and keep private the nonpublic personal and financial information provided to them about Plaintiffs and Class Members.

115. As a direct and proximate result of Defendants' breach of their implied contracts, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

TENTH CAUSE OF ACTION

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

116. The preceding factual statements and allegations are incorporated by reference.

117. Plaintiffs and Class Members conferred a benefit to Defendants in the form of payment for goods and services.

118. Defendants failed to pay for the benefits provided to them by Plaintiffs and Class Members by failing to protect and keep private the nonpublic personal financial information with which Plaintiffs and Class Members entrusted Defendants with.

119. Defendants' failure to pay for the benefits provided to them, *i.e.*, to protect and keep private Plaintiffs and Class Members' nonpublic personal and financial information, was to the detriment of Plaintiffs and Class Members because it was Plaintiffs' and Class Members' nonpublic personal and financial information that was taken by cyber thieves.

120. As a direct and proximate result of Defendants' failure to pay for the benefits provided to them, Plaintiffs and the Class have been harmed and have suffered, and will continue to suffer, damages and injuries, and are entitled to restitution.

ELEVENTH CAUSE OF ACTION

DECLARATORY RELIEF

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

121. The preceding factual statements and allegations are incorporated by reference.

122. An actual controversy has arisen in the wake of the data breach regarding Defendants' duties to safeguard and protect Plaintiffs and Class Members' confidential and sensitive PII. Defendants' PII security measures were (and continue to be) woefully inadequate. Defendants dispute these contentions and contend that their security measures are appropriate.

123. Plaintiffs and Class Members continue to suffer damages, other injury or harm as additional identity theft and identity fraud occurs.

124. Therefore, Plaintiffs and Class Members request a judicial determination of their rights and duties, to ask the Court to enter a judgment declaring, *inter alia*, (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiffs and Class members' confidential and sensitive PII, and timely notify them about the data breach, (ii) Defendants breached (and continue to breach) such legal duties by failing to safeguard and protect Plaintiffs and Class Members' confidential and sensitive PII, and (iii) Defendants' breach of their legal duties directly and proximately caused the data breach, and the resulting damages, injury, or harm suffered by Plaintiffs and Class Members. A declaration from the court ordering the Defendants to stop their illegal practices is required.

TWELFTH CAUSE OF ACTION

NEGLIGENCE/GROSS NEGLIGENCE/NEGLIGENCE PER SE

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

125. The preceding factual statements and allegations are incorporated by reference.

126. Defendants, in offering grocery services and products, knew that Plaintiffs and class members' sensitive PII would be stored or processed by Defendants systems and databases, including in Defendants Hosting. Defendants in fact stored and/or processed this PII through and on its computer systems and/or databases. Plaintiff Jia and many of the class members are a particularly vulnerable and defenseless group of Defendants' users and are more significantly damaged and imminently threatened to be damaged as a result of Defendants' negligence described herein because, without limitation, they are especially: (1) as Chinese immigrants, are attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

127. By collecting, storing, and using this data, Defendants had a duty of care to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting,

and protecting this PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems and data storage architecture to ensure that Plaintiffs' and class members' PII was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Defendants' security systems and data storage architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Defendants' security vulnerabilities and potential compromise of the PII of Plaintiffs and class members; (d) maintaining data security measures consistent with industry standards and applicable state and federal law; and (e) timely and adequately informing Plaintiffs and class members if and when a data breach occurred notwithstanding undertaking (a) through (d) above.

128. Defendants had common law duties to prevent foreseeable harm to Plaintiffs and class members. These duties existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants also knew that it was more likely than not Plaintiffs and other class members would be harmed by such theft.

129. Defendants had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected, stored, and processed by Defendants computer systems.

130. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and class members, on the other hand. The special relationship arose because Plaintiffs and class members entrusted Defendants with their PII by virtue of their participation as customers and immigrants buying services. Defendants alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

131. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 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 PII. Various FTC publications and data

security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

132. Defendants owed heightened duties to Plaintiffs Jia and the Nationwide Minor and California Minor Subclass members, and Defendants was aware of the heightened vulnerability and damage that would be suffered by Plaintiffs Jia and the Nationwide Minor and California Minor Subclass members in the event of a data breach.

133. Defendants knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

134. Defendants knew or should have known that a breach of its systems and data storage architecture would inflict millions of dollars of damages upon Plaintiffs and the Class, and Defendants was therefore charged with a duty to adequately protect this critically sensitive information.

135. Defendants breached the duties it owed to Plaintiffs and class members described above, including the heightened duties owed to Plaintiffs Jia and the Nationwide Minor and California Minor Subclass members, and thus was negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and class members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

136. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and class members, their PII would not have been compromised.

137. As a direct and proximate result of Defendants' negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data

Breach not fully disclosed by Defendants, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

THIRTEENTH CAUSE OF ACTION

CALIFORNIA CONSUMER PRIVACY ACT

Cal. Civ. Code §§ 1798.100 *et seq*.

(On Behalf of Plaintiffs and Each Class Members against all Defendants and DOES 1-100)

138. The preceding factual statements and allegations are incorporated by reference.

139. Plaintiffs and California class members are "consumer[s]" as that term is defined in Cal. Civ. Code. § 1798.140(g). Weee and each DOE Defendant are a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c).

140. Plaintiffs' and Class members' PII is "nonencrypted and nonredacted personal information" as that term is used in Cal. Civ. Code § 1798.150(a)(1). The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1).

141. Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiffs' and California Class Members' PII to protect said PII.

142. Defendants breached the duty they owed to Plaintiffs and California Class Members described above, including the heightened duty owed to Plaintiffs Jia Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and California Class Members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

143. Defendants' breach of the duty they owed to Plaintiffs and the California Class Members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiffs and the Class members suffered damages, as described above and as will be proven at trial.

144. Plaintiffs seek injunctive relief in the form of an order enjoining Defendants from

continuing the practices that constituted their breach of the duty owed to Plaintiffs and Class Members as described above. Concurrently with the filing of this Complaint, Plaintiffs are serving a letter of notice on Weee! pursuant to Cal. Civ. Code § 1798.150(b) and anticipate amending this Complaint to seek statutory damages upon receipt of a written statement from Weee! in response to that letter of notice.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

1) For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and Plaintiffs' counsel to represent the Class as alleged herein;
2) For injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:
    a) Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
    b) Requiring Defendants to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
    c) Requiring Defendants to delete, destroy, and purge the PII of Plaintiffs and class members unless Defendants can provide the Court a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the class members;
    d) Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and class members' PII;
    e) Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
    f) Requiring Defendants to audit, test, and train its personnel regarding any new or modified procedures;

g) Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h) Requiring Defendants to conduct regular database scanning and security checks;

i) Requiring Defendants 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 employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

j) Requiring Defendants to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

k) Requiring Defendants to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l) Requiring Defendants to meaningfully educate all class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

m) Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from its servers, as well as programs sufficient to protect infiltration of Defendants' local servers (or vendor services) connected to Defendants' systems; and

n) Requiring Defendants to provide ten years of identity theft and fraud protection services to Plaintiffs and class members.

3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

4) For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;

5) For an award of restitution or disgorgement, in an amount to be determined;

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

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

Dated: May 11, 2023

Respectfully submitted,

By: */s/ Blake J. Lindemann*

Blake J. Lindemann
California Bar No. 255747
E-mail: blake@lawbl.com
Donna R. Dishbak
California Bar No. 259311
E-mail: donna@lawbl.com
LINDEMANN LAW FIRM, APC
9777 Wilshire Blvd., 4th Floor
Beverly Hills, CA 90212
Telephone No: 310-279-5269
Facsimile No: 310-300-0267

Attorneys for Plaintiff and the Proposed Classes

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all issues, claims, and remedies so triable.

Dated: May 11, 2023

Respectfully submitted,

By: */s/ Blake J. Lindemann*

Blake J. Lindemann
California Bar No. 255747
E-mail: blake@lawbl.com
Donna R. Dishbak
California Bar No. 259311
E-mail: donna@lawbl.com
LINDEMANN LAW FIRM, APC
9777 Wilshire Blvd., 4th Floor
Beverly Hills, CA 90212
Telephone No: 310-279-5269
Facsimile No: 310-300-0267

Attorneys for Plaintiff and the Proposed Classes

ClassAction.org