JS 44 (Rev. 04/21) (TXND 4/21)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

MARIA GOMEZ, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Los Angeles Cnty, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

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

Mark J. Hilliard, LAW OFFICES OF MARK J. HILL, 1233 Alpine Rd., Walnut Creek, CA 94596; (310) 709-9749

DEFENDANTS

Nike, Inc.

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

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Data breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Stacie Beckerman DOCKET NUMBER 3:26-cv-00426

DATE 03/24/26

SIGNATURE OF ATTORNEY OF RECORD /s/Mark Hill

FOR OFFICE USE ONLY

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

Mark J. Hilliard, Esq. (OR S.B. #161922)
THE LAW OFFICES OF MARK J. HILLIARD
1233 Alpine Road
Walnut Creek, California 94596
Telephone: (310) 709-9749
Email: mark.hilliard.esq@gmail.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

*Admitted *Pro hac vice*

Attorneys for Representative Plaintiff Maria Gomez

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON

MARIA GOMEZ, individually, and on behalf of all others similarly situated, Plaintiff, v. NIKE, INC., Defendant.	Case No.: **CLASS ACTION** **COMPLAINT FOR DAMAGES** **[JURY TRIAL DEMANDED]**

Plaintiff Maria Gomez ("Plaintiff"), individually and on behalf of all others similarly situated, and on behalf of the general public, brings this Class Action Complaint, against defendant Nike, Inc. ("Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. Representative Plaintiff Maria Gomez ("Representative Plaintiff") brings this class action against Defendant Nike, Inc. ("Defendant") for its failure to properly secure and safeguard Representative Plaintiff's and/or Class Members' personally identifiable information stored within Defendant's information network, including, without limitation, names, email addresses, billing addresses, phone numbers, transaction information and payment card details (these types of information, inter alia, being thereafter referred to, collectively, as "personally identifiable information" or "PII").[1] All such information is referred to in the aggregate herein as "Private Information."

2. With this action, Representative Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiff and other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on January 21, 2026, by which cybercriminals infiltrated Defendant's inadequately protected network and accessed the Private Information which was being kept there (the "Data Breach").

3. While Defendant claims to have discovered the breach as early as January 21, 2026, Defendant did not begin informing victims of the Data Breach until February 25, 2026, and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

received letters from Defendant informing them of it. The Notice received by Representative Plaintiff was dated February 25, 2026.

4. Defendant acquired, collected and stored Representative Plaintiff's and Class Members' Private Information. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential Private Information.

5. Defendant disregarded the rights of Representative Plaintiff and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiff's and Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

II. THE PARTIES

6. Plaintiff is a citizen and resident of Los Angeles County, California.

7. Defendant is a for-profit enterprise with a principal place of business located in Beaverton, Oregon. Defendant "is a team comprised of the Nike, Jordan and Converse brands[.]"[2]

[2] https://about.nike.com/en/company

8. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

III. JURISDICTION AND VENUE

9. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

10. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts this State.

12. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further 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 Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Belated Notice

13. According to the Breach Notice received by Plaintiff, on or around January 21, 2026, Defendant discovered that an unauthorized party had accessed a portal hosted by a third-party service provider. Based on a subsequent forensic investigation, Nike determined that

cybercriminals infiltrated its inadequately secured computer environment and thereby gained access to its data files. The investigation further determined that, through this infiltration, cybercriminals potentially accessed and viewed files containing the sensitive Private Information of thousands of customers. This information is supported by public reporting covering the Breach[3]

14. Representative Plaintiff and Class Members were required to provide their Private Information to Defendant in order to receive goods. Thus, Defendant created, collected and stored Representative Plaintiff's and Class Members' Private Information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

15. According to the Breach Notice mailed by Defendant, the Private Information accessed by cybercriminals included names, email addresses, billing addresses, phone numbers, transaction information, and payment card information.[4]

16. Despite the sensitivity of the PII that was exposed, and the attendant consequences to affected individuals as a result of the exposure, Defendant failed to disclose the Data Breach for several weeks from the time of the Breach. This inexplicable delay further exacerbated the harms to Plaintiff and Class members.

17. Based on the notice letter received by Plaintiff, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiff's Private Information was stolen in the Data Breach.

[3] *See* https://www.cloaked.com/post/is-your-information-at-risk-in-the-nike-data-breach-heres-what-you-need-to-know
[4] *Id*.

18. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Private Information, viewed the Private Information on Defendant's network, and has engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiff's and Class members' Private Information on the dark web.

19. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiff and Class members' Private Information confidential and to protect such Private Information from unauthorized access.

20. Nevertheless, Defendant failed to spend sufficient resources on encrypting sensitive personal data, preventing external access, detecting outside infiltration, and training its employees to identify hacking threats and defend against them.

21. The stolen Private Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

B. Plaintiff's Experience

22. Plaintiff received a notice letter from Defendant dated February 25, 2026, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

23. Plaintiff is very careful with her Private Information.

24. Plaintiff would not have provided her Private Information to Defendant had she known that Defendant would not utilize standard measures to reasonably secure her sensitive information.

25. Because of the Data Breach, Plaintiff's Private Information is now in the hands of cyber criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

26. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that she is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

27. Plaintiff is very concerned and worried that her Private Information is now in the hand of cybercriminals.

28. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Private Information; and (e) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to

further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

C. Defendant had an Obligation to Protect Private Information under the Law and the Applicable Standard of Care

29. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive Private Information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

30. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class members' Private Information.

31. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and application systems to ensure that the Private Information in its possession was adequately secured and protected.

32. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

33. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its systems in a timely manner.

34. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

35. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust Private Information with Defendant.

36. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

37. Defendant owed a duty of care to Plaintiff and the Class because it was a foreseeable victim of a data breach.

D. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

38. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[5] Yahoo,[6] Marriott International,[7] Chipotle, Chili's, Arby's,[8] and others.[9]

39. Defendant should certainly have been aware, and indeed was aware, that it was at

[5] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[6] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[7] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[8] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[9] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

risk for a data breach that could expose the Private Information that it collected and maintained.

40. Defendant was also on notice of the importance of data encryption of Private Information. Defendant knew it kept Private Information in its systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

E. Cyber Criminals Will Use Plaintiff's and Class Members' Private Information to Defraud Them

41. Plaintiff and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

42. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[10] For example, with the Private Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[11] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

[10] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[11] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

43. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[12]

44. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiff's and the Class members' Private Information on the dark web. The Private Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

45. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[13]

46. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[14]

47. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[15]

---

[12] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

[13] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

[15] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

48. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

49. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[16]

50. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

51. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Private Information;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

[16] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

d. The imminent and certainly impending risk of having their Private Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' Private Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

52. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class members' Private Information.

53. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Private Information Defendant made accessible to

hackers, they are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and all Class members will need to have identity theft monitoring protection for the rest of their lives.

54. None of this should have happened. The Data Breach was preventable.

F. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Private Information

55. Data breaches are preventable.[17] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[18] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[19]

56. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[20]

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

---

[17]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[18]*Id.* at 17.

[19]*Id.* at 28.

[20]*Id.*

58. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.7 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.[21]

59. The FTC further recommends that companies not maintain Private 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 suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the 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.

[21] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

61. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

62. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. Upon information and belief, Frontier failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

64. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiff's and Class Members' Private Information.

65. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class members' Private Information.

66. Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

67. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

68. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Plaintiff's and Class members' Private Information was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

69. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' Private Information from those risks left that information in a dangerous condition.

70. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

71. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

72. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose Private Information was compromised as a result of the Data Breach.

73. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

74. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

75. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

76. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Defendant.

77. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class that Plaintiff seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

78. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of

individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

79. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and Class members' Private Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Private Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continues to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

80. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

81. Defendant solicited, gathered, and stored the Private Information of Plaintiff and the Class as part of the operation of its business and in order to gain revenues.

82. Upon accepting and storing the Private Information of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

83. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

84. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiff and the Class members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

85. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive Private Information.

86. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

87. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard Private Information.

88. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

89. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

90. Defendant breached its duty of care by failing to adequately protect Plaintiff's and Class members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

f. Failing to adequately train its employees to not store Private Information longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Private Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their Private Information.

91. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

92. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

93. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class members while it was within Defendant's possession and control.

94. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps toward securing their Private Information and mitigating damages.

95. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

96. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

97. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

98. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

99. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiff's and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiff therefore is entitled to the evidentiary presumptions for negligence *per se*.

100. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and the Class.

101. 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 Private Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

102. Defendant gathered and stored the Private Information of Plaintiff and the Class as part of its business, which affect commerce.

103. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

104. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' Private Information, and by failing to provide prompt and specific notice without reasonable delay.

105. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

106. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

107. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Private Information.

108. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

109. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

110. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence.

111. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO

BREACH OF IMPLIED CONTRACT

112. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

113. Plaintiff and Class Members were required to provide Defendant with their Private Information in order to receive goods from Defendant.

114. When Plaintiff and Class Members provided their Private Information to Defendant when seeking these services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Private Information and to timely notify them in the event of a Data Breach.

115. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and the Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards.

116. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Private Information, including through industry standard technologies like encryption, and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant *weeks* to warn Plaintiff and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiff and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiff and Class Members unsure as to the extent of the information that was compromised.

117. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential

damages that Defendant knew about when it requested Plaintiff's and the Class Members' Private Information.

COUNT THREE

UNJUST ENRICHEMNT

118. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

119. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

120. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class members as part its business operations and to gain profits. As such, Defendant had direct knowledge of the monetary benefits conferred upon it.

121. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiff's and the Class members' Private Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiff's and Class members' Private Information.

122. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class members.

123. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Private Information, including without

limitation those industry standard data security practices, procedures, and programs discussed herein.

124. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of Private Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

125. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

126. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

COUNT FOUR

VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT, Cal. Civ. Code § 1798.100, et seq. ("CCPA") (On Behalf of Plaintiff and the California Subclass)

127. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

128. Defendant violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent the Personal Information of Plaintiff and the California Subclass from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

129. The non-redacted and non-encrypted Personal Information of Plaintiff and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant' violations of their duty under the CCPA.

130. Plaintiff and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as a direct and proximate result of Defendant' acts described above.

131. Defendant knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the Personal Information so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff and members of the California Subclass was exposed.

132. Defendant is an entity organized for the financial benefit of its owners and collect PII as defined in Cal. Civ. Code § 1798.140.

133. Defendant is a "business" within the meaning of the CCPA, Cal. Civ. Code § 1798.140(c), as it is a legal entity that collects consumers' personal information, determines the

purposes and means of processing that information, conducts business in the State of California, and satisfies at least one of the applicable thresholds under the statute.

134. Plaintiff the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendant still hold PII related to Plaintiff and the California Subclass. Plaintiff and the California Subclass have an interest in ensuring that their PII is reasonably protected.

135. At this time, Plaintiff and California Class Members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

136. Concurrently with the filing of this Complaint, Plaintiff is providing written notice to Defendant identifying the specific provisions of this title he alleges it has violated. If within 30 days of Plaintiff's written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. See Cal. Civ. Code § 1798.150(b).

COUNT FIVE

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80 *et seq*
(On Behalf of Plaintiff and the California Subclass)

137. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

138. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

139. Section 1798.81.5(b) further states that: "[a] 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."

140. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

141. Plaintiff and members of the California Subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

142. The Personal Information of Plaintiff and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collect and which was impacted by the cybersecurity attack includes an individual's name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) social security number; (ii) driver's

license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

143. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California Subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California Subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

144. As a direct and proximate result of Defendant' violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of

Plaintiff and the California Subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

145. As a direct and proximate result of Defendant' acts or omissions, Plaintiff and the California Subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

146. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

147. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then

any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

148. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, Defendant have not sent written notice of the data breach to all impacted individuals. As a result, Defendant have violated § 1798.82 by not providing legally compliant and timely notice to Plaintiff and class members. Defendant identified the Data Breach on October 11, 2024.

Nevertheless, Defendant failed to timely disclose the Breach of Plaintiff and Class members until November 15, 2024, or later. Plaintiff and class members could have taken action to protect their personal information during this long period but were unable to do so because they were not timely notified of the Breach.

149. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and Class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

150. As a direct consequence of the actions as identified above, Plaintiff and the California Subclass members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT SIX

DECLARATORY JUDGMENT/INJUNCTIVE RELIEF

151. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

152. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

153. Defendant owes duties of care to Plaintiff and Class Members that require Defendant to adequately secure their Private Information.

154. Defendant still possess Plaintiff's and Class Members' Private Information.

155. Defendant do not specify in the notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

156. Plaintiff and Class Members are at risk of harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

157. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' Private Information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

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

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

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

v. Ordering that Defendant cease transmitting Private Information via unencrypted email;

vi. Ordering that Defendant cease storing Private Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and Private Information to

third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

DATED: March 24, 2026

/s/ Mark J. Hilliard
Mark J. Hilliard, Esq. (OR S.B. #161922)
THE LAW OFFICES OF MARK J. HILLIARD
1233 Alpine Road Walnut Creek, California 94596
Telephone: (310) 709-9749 Email:
mark.hilliard.esq@gmail.com

A. Brooke Murphy
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

Counsel for Plaintiff and the Proposed Class