Tina Wolfson (SBN 174806)
*twolfson@ahdootwolfson.com*
Robert Ahdoot (SBN 172098)
*rahdoot@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310-474-9111
Facsimile: 310-474-8585

John J. Nelson (SBN 317598)
*jnelson@milberg.com*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC**
280 South Beverly Drive
Beverly Hills, CA 90212
Telephone: 858-209-6941

*Attorneys for Plaintiff and the Proposed Class*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

MALCOLM SCOTT, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SALESFORCE, INC., and DOES 1-100, inclusive,

Defendants.

Case No. 3:25-cv-7232

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Malcom Scott ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), by and through his undersigned counsel, brings this class action complaint against Defendants Salesforce, Inc. ("Salesforce") and Does 1-100 (collectively, "Defendants"). Plaintiff brings these allegations on information and belief, except the allegations specifically pertaining to himself, which are based on his personal knowledge. individually and on behalf of all others similarly situated ("Class members").

## NATURE OF THE ACTION

1. Plaintiff brings this class action individually and on behalf of all other individuals who had their sensitive personal information, including, at minimum, names, addresses, dates of birth, driver's license numbers, and/or partial Social Security numbers (collectively, "Personal Information") disclosed to unauthorized third parties during a data breach compromising Salesforce in or around May 2025 (the "Data Breach").

2. Salesforce is a cloud-based software company providing its services to various corporate clients throughout the country in sales, customer service, marketing automation, e-commerce, analytics, artificial intelligence, and application development.

3. On May 30, 2025, Farmers Group, Inc. ("Farmers"), one of the country's largest insurance companies, discovered suspicious activity involving an unauthorized actor accessing one of its third-party vendor's databases containing Farmers customer information.[1] On information and belief, that third-party vendor is Salesforce, whose software was reportedly targeted through compromised customer OAuth tokens, and/or phishing attempts utilizing fake Salesforce apps to obtain victims' login details.[2]

[1] *See* Farmers Notice of Security Incident, available at https://www.farmers.com/content/dam/farmers/marketing/digital/aem/pdfs/disclosures/notice-of-incident.pdf (last accessed August 27, 2025).

[2] *See* Widespread Data Theft Targets Salesforce Instances via Salesloft Drift, available at https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift (last accessed August 27, 2025); https://www.bleepingcomputer.com/news/security/farmers-insurance-data-breach-impacts-11m-people-after-salesforce-attack/ (last accessed August 27, 2025); https://www.scworld.com/brief/over-1-1m-farmers-insurance-customers-impacted-by-salesforce-linked-hack (last accessed August 27, 2025).

4. This is a "hub-and-spoke" data breach case. The "hub" in this case is Salesforce, which is a company that specializes in cloud-storage technologies to warehouse and secure sensitive data, as well as other software products. Salesforce sells its software services to numerous companies, or "spokes," who store information using Salesforce's cloud-based software. These spokes includes Farmers and numerous other entities, the names of which are not yet known but are included as Doe Defendants 1-100. All allegations regarding Defendants generally include and apply to each and every one of the "spoke" Doe Defendants.

5. According to the Notice of Security Incident published on Farmers' website, "the third-party vendor had monitoring tools in place, which allowed the vendor to quickly detect the activity and take appropriate containment measures, including blocking the unauthorized actor."

6. The Data Breach reportedly impacted approximately 1.1 million Farmers' customers.[3] On information and belief, the number of affected individuals across all of Salesforce's clients is much larger.

7. Though Farmers represents it "takes protecting your personal information seriously" it provides a paltry amount of information concerning the breach on its website and does not position impacted customers to protect themselves against fraud and identity theft. Indeed, the website is clear that its customers (and perhaps others) may already be experiencing the fallout of the Data Breach, as it has provided a customer care toll-free number for customers to call with questions about the Data Breach.

8. Defendants were well aware of or should have known of their data security shortcomings. Defendants collect and maintain sensitive Personal Information about their customers and potential customers, including drivers' license numbers and Social Security numbers ("SSNs"), along with other highly sensitive information. Defendants require customers to provide this information in connection with using their services.

[3] https://www.bleepingcomputer.com/news/security/farmers-insurance-data-breach-impacts-11m-people-after-salesforce-attack/ (last accessed August 27, 2025).

9. Defendants' failures to ensure that their servers and systems were adequately secure fell far short of their obligations and Plaintiff's and Class members' reasonable expectations for data privacy jeopardized the security of Plaintiff's and Class member's Personal Information, and exposed Plaintiff and Class members to fraud and identity theft or the serious risk of fraud and identity theft.

10. As a result of Defendants' conduct and the resulting Data Breach, Plaintiff and Class members' privacy has been invaded, their Personal Information is now in the hands of criminals, they have either suffered fraud or identity theft, or face an imminent and ongoing risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

## PARTIES

11. Plaintiff Malcolm Scott is a resident of Tampa, Florida. Plaintiff had an account with Farmers and/or its affiliates. Believing Farmers' data vendors, like Salesforce, would implement and maintain reasonable security and practices to protect customer Personal Information, Plaintiff provided Personal Information to Farmers in connection with seeking insurance products and services from, and transacting with, Farmers.

12. Defendant Salesforce, Inc. is a corporation organized under the laws of the state of Delaware, with a principal place of business located in San Francisco, California. Salesforce provides a wide range of software products to companies in various industries.

13. Plaintiff does not know the true names and capacities of the Doe Defendants, and therefore sue them by fictitious names. When their true names and capacities are discovered, Plaintiff will seek leave to amend this complaint by inserting those true names and capacities. On information and belief, 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, and/or all other types of entities and/or individuals as discovery in the matter may reveal. Regardless, Plaintiff alleges that each of the Doe Defendants is legally responsible for the Data Breach and legally caused and/or was a substantial factor in the injury and damages to Plaintiff and Class members.

## JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class members, the action is a class action in which one or more Class members are citizens of states different from Defendants.

15. The Court has personal jurisdiction over Defendant Salesforce and the Doe Defendants because Salesforce maintains its headquarters and principal places of business in this District and conducts significant business in this District, thus availing itself of California's markets by providing its software services therein; it has sufficient minimum contacts with California; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District.

16. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in, were directed to, and/or emanated from this District; Defendants transact substantial business and have agents in this District; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District; and because Defendant Salesforce's corporate headquarters are located within this District.

## FACTUAL ALLEGATIONS

### A. Salesforce and the Doe Defendants Collect and Store Personal Information

17. In providing its software services to businesses, Salesforce routinely collects sensitive Personal Information of its clients' customers and consumers. It asserts on its website that "We earn the trust of our customers, employees, and extended family through transparency, security, compliance, privacy, and performance. And we deliver the industry's most trusted infrastructure."[4] Salesforce is aware of the sensitive nature of the Personal Information it collects, and it acknowledges the importance of data privacy. The same is true of the Doe Defendants who provided their customers' Personal Information to Salesforce.

[4] https://trust.salesforce.com/ (last accessed August 27, 2025).

18. This information includes, on information and belief, "phone book" information such as names, email addresses, phone numbers, mailing addresses, but also includes highly sensitive information including SSNs, financial information, tax information, credit history, employment information, drivers' license information, insurance information, and other highly sensitive information. Some or all of this information is typically provided to a business when a consumer is attempting to secure products and services. As a result, software providers like Salesforce collect and maintain large amounts of highly sensitive Personal Information received and stored through its various business clients.

19. Salesforce's public-facing statements on privacy and security, much like similar statements made by Doe Defendants[5] make it clear that it is aware of the need to safeguard the sensitive Personal Information entrusted to it by clients and consumers as part of providing its software services.

**B. The Data Breach**

20. On May 30, 2025, Farmers discovered suspicious activity involving an unauthorized actor accessing one of Farmers' third-party vendor's databases containing Farmers customer information.[6]

21. According to the Notice of Security Incident published on Farmers' website, "the third-party vendor had monitoring tools in place, which allowed the vendor to quickly detect the activity and take appropriate containment measures, including blocking the unauthorized actor."

22. Farmers launched an investigation to determine the nature and scope of the incident and notified appropriate law enforcement authorities. That investigation revealed that "an unauthorized actor accessed the vendor's database on May 29, 2025, and acquired certain data."[7]

[5] For example, in Farmers' Privacy Notice on its website, it represents: "our customers are our most valued assets. Protecting your privacy is important to us." https://www.farmers.com/about-us/ (last accessed August 27, 2025).

[6] *See* Farmers Notice of Security Incident, available at https://www.farmers.com/content/dam/farmers/marketing/digital/aem/pdfs/disclosures/notice-of-incident.pdf (last accessed August 27, 2025).

[7] *Id.*

23. According to Farmers, it began sending written notices to affected individuals on August 22, 2025, approximately three months after first learning about the Data Breach.[8] On information and belief, the "vendor" repeatedly referenced by Farmers as the source of the Data Breach is Salesforce, which has affected numerous other "spoke" businesses as well who use Salesforce's software and services.

### C. Impact of the Data Breach

24. The actual extent and scope, and the impact, of the Data Breach on Defendants' customers (or other affiliated persons) remains uncertain. Unfortunately for Plaintiff and Class members, the damage is already done because their sensitive Personal Information is confirmed by at least one spoke company, Farmers, to have been disclosed to unauthorized persons during the Data Breach.

25. Defendants knew or should have known that their IT systems and/or servers are unsecure and do not meet industry standards for protecting highly sensitive customer Personal Information. On information and belief, Defendants failed to timely make changes to their data security systems, privacy policies, and their IT systems and servers, exposing their customers' Personal Information to the risk of theft, identity theft, and fraud.

26. Some of the harm caused to Plaintiff and Class members by the Data Breach has already been suffered, with additional harm imminent in the wake of the Data Breach.

27. The Data Breach creates a heightened security concern for Plaintiff and Class members because their SSNs, financial information, and other sensitive information was potentially disclosed. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

28. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to

[8] *Id.*

the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[9] TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[10]

29. In addition, threat actors seek out driver's license numbers because they are highly valuable pieces of personal information. A driver's license number can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[11] Driver's license numbers are particularly useful to identity thieves for applying for unemployment or other government benefits.

30. Defendants had a duty to keep Plaintiff's and Class members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class members provided their Personal Information to Defendants with the understanding that Defendants would comply with their privacy and data security representations and obligations to keep such information confidential and secure from unauthorized disclosures.

31. Defendants' data security obligations were particularly important given the substantial increase in data breaches in recent years, which are widely known to the public and to anyone in Defendants' industry. In particular, Salesforce's entire business model is based on providing secure cloud-based software to its customers.

[9] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

[10] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[11] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach,* FORBES (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=146576a68658.

**D. Theft of Personal Information Has Serious Consequences for Victims**

32. Data breaches are by no means new and they should not be unexpected. Business Insider has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[12] It is well known amongst companies that store sensitive personally identifying information that sensitive Personal Information—like SSNs, financial information, tax information, etc.—is valuable and frequently targeted by criminals.

33. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, like Farmers, and these companies must ensure that data privacy and security practices and protocols are adequate to protect against and prevent known and expected attacks.

34. Theft of Personal Information is serious. The Federal Trade Commission has warned consumers that identity thieves use Personal Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[13]

35. Indeed, with access to an individual's Personal Information, criminals can do more than simply empty a victim's bank account. They can also commit all manner of fraud, including: obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; obtain lending or lines of credit; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[14]

---

[12] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed Jan. 23, 2024).

[13] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Jan. 23, 2024).

[14] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Jan. 23, 2024).

36. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[15]

37. Personal Information is a valuable property right.[16] The value of sensitive personal information as a commodity is measurable.[17] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[18]

38. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs, financial information, driver's license numbers, and other Personal Information directly on various illegal websites making the information publicly available, often for a price. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[15] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Jan. 23, 2024).

[16] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[17] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[18] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

39. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

40. Consumers place a high value on the privacy of sensitive data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[19]

41. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[20]

42. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

43. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[21]

44. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

[19] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[20] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[21] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

**E. Defendants Failed to Act in the Face of a Known Risk of a Data Breach**

45. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect Personal Information, leaving their customers and clients (and potentially others) exposed to risk of fraud and identity theft.

46. Defendants are, and at all relevant times have been, aware that the sensitive Personal Information they handle and store is highly sensitive. As companies that require highly sensitive and identifying information in connection with providing their products and services, Defendants are aware of the importance of safeguarding that information and protecting their systems and products from security vulnerabilities.

47. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and were alerted to the risk associated with failing to ensure that Personal Information was adequately secured.

48. Despite the well-known risks of hackers and cybersecurity intrusions, Defendants failed to employ (and/or failed to ensure its third-party vendors employed) adequate data security measures or in a meaningful way in order to prevent breaches, including the Data Breach.

49. The security flaws inherent to Defendants' and their vendors' IT systems or servers run afoul of industry best practices and standards. Had Defendants adequately protected and secured their servers or systems, and the sensitive Personal Information stored therein, Defendants could have prevented the Data Breach.

50. Despite that Defendants were on notice of the very real possibility of data theft, Defendants permitted a massive intrusion to occur that resulted in disclosure of Plaintiff's and over one million other Class members' Personal Information to criminals.

51. Defendants permitted Class members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

52. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen

through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[22]

53. As a result of the events detailed herein, Plaintiff and Class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

54. Victims of the Data Breach have likely already experienced harms and are subject to an imminent and ongoing risk of harm, including identity theft and fraud.

55. As a result of Defendants' failure to ensure that the impacted systems and servers were protected and secured, the Data Breach occurred. As a result of the Data Breach, Plaintiff's and Class members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

## CLASS ALLEGATIONS

56. Plaintiff brings this action individually and on behalf of the following Class pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> All residents of the United States who were impacted by the Salesforce Data Breach, including all persons who were sent notice by Farmers or any other client of Salesforce that their Personal Information was compromised as a result of the Data Breach.

57. Excluded from the Class are: (1) any Judge presiding over this action, members of their immediate families, and Court Staff; and (2) Defendants, their subsidiaries, parent companies,

[22] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 30, 2017), https://www.reuters.com/article/idUSKBN18M2BY/.

successors, predecessors, and any entity in which Defendants, or their parents, have a controlling interest, and their current or former officers and directors.

58. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include over one million members who are geographically dispersed.

59. **Typicality**: Plaintiff's claims are typical of Class members' claims. Plaintiff and all Class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class members they seek to represent. Accordingly, Plaintiff's claims are typical of Class members' claims.

60. **Adequacy**: Plaintiff's interests are aligned with the Class Plaintiff seeks to represent, and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and undersigned counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

61. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class member's claims. 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 Class members individually to effectively redress Defendants' 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 the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

62. **Commonality and Predominance:** The following questions common to all Class members predominate over any potential questions affecting individual Class members:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants' data security practices resulted in the disclosure of Plaintiff's

and other Class members' Personal Information and the Data Breach;

- whether Defendants violated privacy rights and invaded Plaintiff's and Class members' privacy; and
- whether Plaintiff and Class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

63. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

64. **Injunctive and Declaratory Relief:** Consistent with Fed. R. Civ. P. 23(b)(2), Defendants, through their 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.

## CAUSES OF ACTION

### COUNT I
### Negligence

65. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

66. Defendants were entrusted with, stored, and otherwise had access to the Personal Information of Plaintiff and Class members.

67. Defendants knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiff and Class members, and to not ensuring that their or their vendors' servers and systems, and the Personal Information, were secure. These risks were reasonably foreseeable to Defendants.

68. Defendants owed duties of care to Plaintiff and Class members whose Personal Information had been entrusted to them.

69. Defendants breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate data security. Defendants had a duty to safeguard Plaintiff's and Class members' Personal Information and to ensure that they adequately protected Personal Information. Defendants breached this duty.

70. Defendants' duty of care arises from its knowledge that its customers entrust it with highly sensitive Personal Information that Defendants is required to, and represents that it will, handle securely. Indeed, Defendants commit to data privacy on their websites and privacy notices, including safeguarding sensitive Personal Information.

71. Only Defendants were in a position to ensure that their and their vendor's systems, servers, and services were sufficient to protect against breaches and the harms that Plaintiff and Class members have now suffered.

72. A "special relationship" exists between Defendants, on the one hand, and Plaintiff and Class members, on the other hand. Defendants entered into a "special relationship" with Plaintiff and Class members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiff and Class members in connection with their attempts or efforts to obtain Defendants' products and services.

73. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

74. Defendants acted with wanton disregard for the security of Plaintiff's and Class members' Personal Information.

75. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendants' breach of duties. Defendants knew or should have known it was failing to meet these duties, and that Defendants' breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Personal Information.

76. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have been harmed and face an imminent and ongoing risk of harm.

77. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT II**
**Negligence Per Se**

78. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

79. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and Class members' Personal Information.

80. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide adequate data security practices to safeguard Plaintiff's and Class members' Personal Information.

81. Defendants breached its duties to Plaintiff and Class members under the Federal Trade Commission Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*) ("GLBA"), the Driver's Privacy Protection Act, 18 U.S.C. §§ 2724, *et seq.* ("DPPA"), among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale of products and services in order to safeguard Plaintiff's and Class members' Personal Information.

82. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

83. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

84. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendants' breach of duties. Defendants knew or should have known that they were failing to meet their duties, and that a breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Personal Information.

85. As a direct and proximate result of Defendants' negligence per se, Plaintiff and Class members have been harmed and face an imminent and ongoing risk of harm.

86. As a direct and proximate result of Defendants' negligence per se, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT III**
**Breach of Implied Contract**

87. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

88. Defendants provided or provides products and services to Plaintiff and Class members,

or Plaintiff and Class members provided their Personal Information to Defendants as prospective customers or in some other capacity.

89. In connection with their business relationship, Plaintiff and Class members entered into implied contracts with Defendants.

90. Pursuant to these implied contracts, Plaintiff and Class members provided Defendants with their Personal Information. In exchange, Defendants agreed, among other things: (1) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' Personal Information; and (2) to protect Plaintiff's and Class members' Personal Information in compliance with federal and state laws and regulations and industry standards.

91. The protection of Personal Information was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Had Plaintiff and Class members known that Defendants would not adequately protect its customers' Personal Information they would not have done business with Defendants.

92. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their Personal Information.

93. Necessarily implicit in the agreements between Plaintiff/Class members and Defendants was Defendants' obligation to take reasonable steps to secure and safeguard Plaintiff's and Class members' Personal Information.

94. Defendants breached their obligations under their implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect their Personal Information.

95. Defendants' breach of their obligations of their implied contracts with Plaintiff and Class members directly resulted in the Data Breach.

96. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of Defendants' material breaches of its agreements.

97. Plaintiff and other Class members were damaged by Defendants' breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for

which they are entitled to compensation; (iii) their Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established national and international market; (vi) they were deprived of the benefit of their bargain; and/or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

**COUNT IV**
**Breach of Fiduciary Duty**

98. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

99. A relationship existed between Plaintiff and Class members and Defendants in which Plaintiff and Class members put their trust in Defendants to protect the Personal Information of Plaintiff and Class members and Defendants accepted that trust.

100. Defendants breached the fiduciary duties that they owed to Plaintiff and Class members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the Personal Information of Plaintiff and Class members.

101. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and Class members.

102. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and Class members would not have occurred.

103. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class members.

104. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages, and injunctive relief.

**COUNT V**
**Invasion of Privacy (Intrusion Upon Seclusion)**

105. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

106. Plaintiff and Class members had a reasonable expectation of privacy in the Personal Information that Defendants disclosed without authorization.

107. By failing to keep Plaintiff's and Class members' Personal Information safe, knowingly employing inadequate data privacy policies and protocols, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class members' privacy by, *inter alia*:

a. intruding into Plaintiff's and Class members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiff's and Class members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure Personal Information from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiff's and Class members' Personal Information without consent.

108. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class members' position would consider its actions highly offensive.

109. Defendants knew that their IT systems and servers were vulnerable to data breaches prior to the Data Breach.

110. Defendants invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

111. As a proximate result of such unauthorized disclosures, Plaintiff's and Class members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

112. In failing to protect Plaintiff's and Class members' Personal Information, and in disclosing Plaintiff's and Class members' Personal Information, Defendants acted with malice and

oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private.

113. Plaintiff seeks injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

**COUNT VI**
**Unjust Enrichment**

114. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

115. This claim is pleaded in the alternative to the implied contract claim.

116. Defendants have profited and benefited from the monies or fees paid and the Personal Information provided by Plaintiff and Class members to receive services from Defendants.

117. Defendants have voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiff and Class members did not receive services of the quality, nature, fitness, or value represented by Defendants and that reasonable consumers expected.

118. Defendants have been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiff and Class members.

119. Equity and justice militate against permitting Defendants to retain these profits and benefits.

120. Plaintiff and Class members suffered injury as a direct and proximate result of Defendants' unjust enrichment and seek an order directing Defendants to disgorge these benefits and pay restitution to Plaintiff and Class members.

**COUNT VII**
**Violations of the California Unfair Competition Law,**
**Bus. & Prof. Code §§ 17200, *et seq.* (the "UCL")**

121. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

122. Defendants' conduct constitutes unfair, illegal, and fraudulent business practices within

the meaning of the California Business & Professions Code § 17200, *et seq.* (the "UCL").

123. Defendants' conduct violated certain laws as alleged herein, including the Federal Trade Commission Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*) ("GLBA"), and the Driver's Privacy Protection Act, 18 U.S.C. §§ 2724, *et seq.* ("DPPA"). By engaging in the said conduct in the course of doing business within California, Defendants engaged in unlawful business practices in violation of the UCL as to Plaintiff and all Class members.

124. By engaging in the above-described conduct in the course of doing business, Defendants engaged in unfair business practices in violation of the UCL because the harm to Plaintiff and Class Members outweighed any utility that Defendants' conduct may have produced.

125. Defendants' failure to disclose information concerning the Data Breach directly and promptly to affected customers constitutes a fraudulent act or practice in violation of the UCL. Defendants' failure to adequately protect Plaintiff's and Class members' Private Information, despite assurances they would do so and that Defendants met industry standards for data security, also constitutes a fraudulent act or practice in violation of the UCL.

126. Plaintiff and Class Members suffered injury in fact as a result of Defendants' conduct.

127. Individually and on behalf of the Class, Plaintiff seeks injunctive relief, restitution, and all other damages available under this cause of action.

**COUNT VIII**
**Violations of the Driver's Privacy Protection Act,**
**18 U.S.C. §§ 2724, *et seq.* (the "DPPA")**

128. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

129. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains . . . ." 18 U.S.C. § 2724.

130. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

131. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Driver's license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

132. Pursuant to the allegations herein, Defendants knew or should have known that they obtained, disclosed or re-disclosed, and used PII from a motor vehicle record for a purpose not permitted under the DPPA.

133. By engaging in the conduct described above, Defendants knowingly obtained personal information for a purpose not permitted under the DPPA.

134. By engaging in the conduct described above, Defendants knowingly used personal information for a purpose not permitted under the DPPA.

135. By engaging in the conduct described above, Defendants knowingly disclosed or re-disclosed personal information for a purpose not permitted under the DPPA.

136. As a result of Defendants; acquisition, use, subsequent Data Breach, and violations of the DPPA, Plaintiff and putative Class members are entitled to statutory damages to maximum allowable, actual damages, liquidated damages, and attorneys' fees and costs.

**PRAYER FOR RELIEF**

Plaintiff, individually and on behalf of the Class, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class members such other favorable relief as allowable under law or at equity.

**JURY TRIAL DEMANDED**

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

Dated: August 27, 2025

Respectfully submitted,

*/s/ Tina Wolfson*

Tina Wolfson (SBN 174806)
*twolfson@ahdootwolfson.com*
Robert Ahdoot (SBN 172098)
*rahdoot@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

Bradley K. King (SBN 274399)
*bking@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
521 Fifth Avenue, 17th Floor
New York, NY 10175
Telephone: 917.336.0171
Facsimile: 917.336.0177

John J. Nelson (SBN 317598)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC**
280 South Beverly Drive
Beverly Hills, CA 90212
Telephone: 858-209-6941
jnelson@milberg.com

Gary M. Klinger (*pro hac vice* forthcoming)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

William "Billy" Peerce Howard (*pro hac vice* forthcoming)
**THE CONSUMER PROTECTION FIRM, PLLC**
401 East Jackson Street, Suite 2340
Truist Place
Tampa, FL 33602
Telephone: 813-500-1500
billy@TheConsumerProtectionFirm.com

*Attorneys for Plaintiff and the Proposed Class*