Colleen L. Fewer (SBN 323808)
BERGER MONTAGUE PC
505 Montgomery Street Suite 625
San Francisco, CA 94111
Tel. 415-376-2097
F. 215-875-4604
cfewer@bergermontague.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STACI JOHNSON, individually and on behalf of all others similarly situated, Plaintiff, v. SALESFORCE, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Staci Johnson ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Salesforce, Inc. ("Salesforce", or "Defendant") and alleges as follows based on personal knowledge as to her own acts and on investigation conducted by counsel as to all other allegations:

I. INTRODUCTION

1. Data breaches are preventable and occur due to the lack of attention and resources that companies like Defendant expend on protecting the highly sensitive information they are entrusted with.

2. Plaintiff brings this class action against Defendant for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") in connection with a data security event disclosed by Defendant in or about July 2025 (the "Data Breach").

3. The PII appears to have included names, Social Security numbers, billing addresses phone numbers, email addresses and dates of birth.[1]

4. Defendant failed to comply with industry standards to protect information systems that contain PII. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the Data Breach in the future.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' PII with which it was entrusted to protect.

6. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure PII from those risks left that property in a dangerous condition.

7. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely

[1] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (Last visited Sept. 8, 2025)

available software able to detect and prevent this type of attack, (9) failing to adequately vet and continuously monitor its third-party vendors for compliance with cybersecurity best practices; (10) failing to implement and execute an adequate comprehensive vender risk management (VRM) program; and (11) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' PII and failing to take standard and reasonably available steps to prevent the Data Breach.

9. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the PII. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the PII of Plaintiff and Class Members.

10. Plaintiff's and Class Members' identities are now at high risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves.

11. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts and credit reports to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

12. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is hard evidence that the Plaintiff's and Class Members' PII was targeted, accessed, has been misused.

13. Plaintiff and Class Members must now closely monitor their financial accounts and credit reports to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

14. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their PII; and (f) the continued risk to their sensitive PII, 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 what it collected and maintained.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of Plaintiff and all similarly situated individuals whose PII was accessed during the Data Breach.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

17. The exposure of one's PII to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff and the Class's PII was exactly that—private. Not anymore. Now, their PII is forever exposed and unsecure.

II. PARTIES

A. Plaintiff

18. Plaintiff Johnson is a citizen and resident of Florida.

B. Defendant Salesforce

19. Defendant Salesforce is a corporation with its principal place of business located in San Francisco, California. Defendant conducts business throughout this District, and nationwide.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, the number of Class Members is numerous, with many members of whom have different citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has personal jurisdiction because Defendant maintains its principal place of business in this District, regularly conduct business in this District, and has sufficient minimum contacts in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District and maintains Plaintiff's and Class Members' PII in this District.

IV. FACTUAL ALLEGATIONS

A. Overview of Defendant

23. Salesforce is a cloud-based software company that provides various services to corporate clients.

24. One of Salesforce's clients is TransUnion, a credit reporting agency.[2]

[2] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (last visited Sept. 15, 2025)

25. Defendant collected and stored Plaintiff's and the proposed Class Members' PII on its information technology computer systems.

26. Defendant made promises and representations to individuals, including Plaintiff and Class Members, that the PII collected from them would be kept safe and confidential, and that the privacy of that information would be maintained. For instance, Defendant's website states as follows "Salesforce has security built into every layer of the Platform. The infrastructure layer comes with replication, backup, and disaster recovery planning. Network services have encryption in transit and advanced threat detection. Our application services implement identity, authentication and user permissions.[3]

27. Large companies like Defendant have an interest in maintaining the confidentiality of the PII entrusted to them, and they are well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding PII in their possession.

28. Defendant represented to consumers and the public that it possesses robust security features to protect PII and that it takes their responsibility to protect PII seriously.

29. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. As a result of collecting and storing the PII of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' PII from disclosure to third parties.

B. The Data Breach

31. On or about, July 28, 2025, an unauthorized third party gained access to Salesforce's system.[4]

[3] https://www.salesforce.com/privacy/products/ (last visited Sept. 15, 2025)

[4] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (last visited Sept. 8, 2025).

32. Attackers gained access to Salesforce's systems by first breaching the GitHub of Salesloft, a third-party sales engagement platform in March 2025. Salesloft's Drift platform is a tool that integrates with Salesforce. The breach of Salesloft's GitHub lead to the theft of Drift OAuth tokens that were later used to gain access to Salesforce data. [5]

33. As a result of this breach of Salesforce's systems, companies that use Salesforce's services in the ordinary course of business (including but not limited to TransUnion) had their customers' sensitive PII compromised in the data breach ("Data Breach"). For instance, the Data Breach compromised the PII of over 4.4 million TransUnion customers in the United States.[6]

34. Defendant knew (or should have known) of the recent increase in similar data breaches.[7] In fact, Google's Threat Intelligence Group warned that threat actors tracked as UNC6040 were targeting Salesforce customers in social engineering attacks.[8]

35. On July 26, 2025, TransUnion publicly reported the Data Breach to the Office of the Maine Attorney General.[9] In its notice letters to impacted individuals, such as Plaintiff, TransUnion stated that there was a "cyber incident involving unauthorized access to some of your personal data that was stored on a third-party application." Multiple articles have reported that the third party is Salesforce.[10]

36. The Data Breach compromised the following information:

---

[5] https://www.bleepingcomputer.com/news/security/salesloft-march-github-repo-breach-led-to-salesforce-data-theft-attacks/ (last visited Sept. 8, 2025).

[6] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (last visited Sept. 15, 2025).

[7] *Id*.

[8] https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/ (last visited Sept. 8, 2025).

[9] https://www.itpro.com/security/data-breaches/transunion-breach-what-can-customers-do (last visited Sept. 8, 2025).

[10] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (last visited Sept. 16, 2025); https://www.cnet.com/tech/services-and-software/more-than-4-4-million-exposed-in-credit-bureau-transunion-breach/ (last visited Sept. 16, 2025); https://www.foxnews.com/tech/transunion-becomes-latest-victim-major-wave-salesforce-linked-cyberattacks-4-4m-americans-affected?msockid=05e3fa24060d6c641080efec07996db0 (last visited Sept. 16, 2025)

- Full names
- Social Security numbers (SSNs)
- Billing addresses
- Dates of birth
- Phone numbers
- Email addresses[11]

37. Defendant failed to prevent the Data Breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

38. The PII that Defendant allowed to be exposed in the Data Breach are the types of private information that Defendant knew or should have known would be the target of cyberattacks.

39. The U.S. Federal Trade Commission ("FTC") directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[12] Immediate notification of a data breach is critical so that those impacted can take measures to protect themselves.

C. Plaintiff's Experience

40. Plaintiff Johnson's PII was held by TransUnion.

41. TransUnion sent Plaintiff Johnson a letter dated August 26, 2025, informing her that her PII was compromised in the Data Breach (the "Letter"). The Letter states that there was a

"cyber incident involving unauthorized access to some of your personal data that was stored on

[11] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (last visited Sept. 8, 2025)

[12] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited Sept. 11, 2025).

a third-party application." As alleged above, the "third-party application" referenced in the letter is Salesforce's application.[13]

42. The Letter suggests that Plaintiff enroll in TransUnion's own credit monitoring service.

43. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred.

44. Plaintiff Johnson is very careful about sharing her sensitive PII and diligently maintains her PII in a safe and secure manner. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

45. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has experienced stress, anxiety, and increased concerns for the loss of her PII and privacy. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff cannot be undone.

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

47. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of cybercriminals.

[13] https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/ (last visited Sept. 16, 2025); https://www.cnet.com/tech/services-and-software/more-than-4-4-million-exposed-in-credit-bureau-transunion-breach/ (last visited Sept. 16, 2025); https://www.foxnews.com/tech/transunion-becomes-latest-victim-major-wave-salesforce-linked-cyberattacks-4-4m-americans-affected?msockid=05e3fa24060d6c641080efec07996db0 (last visited Sept. 16, 2025)

48. Future identity theft monitoring is not only reasonable and necessary—but was suggested by Defendant—and such services will include future costs and expenses. Defendant has only offered its credit monitoring services for 24 months.

49. Plaintiff has a continuing long-term interest in ensuring that her PII, which, upon information and belief, remains in Defendant's control, is protected, and safeguarded from future breaches.

D. Injuries to Plaintiff and Class Members

50. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff and Class members' PII, Plaintiff and Class members have been injured.

51. Plaintiff and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

52. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[14]

53. In addition to fraudulent charges and damage to their credit, Plaintiff and Class members may spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing

[14] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf. (last visited Sept. 11, 2025)

credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

54. Additionally, Plaintiff and Class members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value or use of their PII, and the loss of privacy.

E. Securing PII and Preventing Breaches

55. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

56. Defendant's negligence in safeguarding the PII of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

57. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class members from being compromised.

58. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id*.

59. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

F. The Value of PII

60. It is well known that PII, and Social Security numbers are an invaluable commodity and a frequent target of hackers.

61. People place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[17]

62. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[18] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[19]

63. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40

[17] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf. (last visited Sept. 11, 2025)

[18] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html. (last visited Sept. 11, 2025)

[19] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited Sept. 11, 2025)

to $200, and bank details have a price range of $50 to $200.[20] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

64. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

65. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

66. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link

---

[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/. (last visited Sept. 11, 2025)

[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, June 30, 2025, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (last visited Sept. 11, 2025)

[22] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited Sept. 11, 2025)

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

67. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

68. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[25]

69. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

70. The fraudulent activity resulting from the Data Breach may not come to light for years.

71. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

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

[24] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft. (last visited Sept. 11, 2025)

[25] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html. (last visited Sept. 11, 2025)

years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

72. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

73. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

74. Defendant knew of the unique type and the significant volume of data contained in the PII that Defendant stored on its networks, and, thus, the significant number of individuals who would be harmed by the exposure of the data.

75. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

G. Industry Standards for Data Security

76. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[27]

77. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, Capital One, and Aflac, Defendant knew of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

---

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf. (last visited Sept. 11, 2025)

[27] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view. (last visited Sept. 11, 2025)

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

79. Security standards commonly accepted among businesses that store PII using the Internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

80. The FTC publishes guides for businesses for cybersecurity[28] and protection of PII[29] which includes basic security standards applicable to all types of businesses.

81. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

[28] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. (last visited Sept. 11, 2025)

[29] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited Sept. 11, 2025)

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

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

Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[30]

83. Because Plaintiff and Class members entrusted Defendant with PII, Defendant had a duty to keep the PII secure.

84. Plaintiff and Class members reasonably expect that when their PII is provided to a sophisticated business for a specific purpose, that business will safeguard their PII and use it only for that purpose.

85. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

H. CLASS ALLEGATIONS

86. This action is brought as a class action pursuant to Federal Rule of Civil Procedure 23.

87. Plaintiff brings this action on behalf of herself and the following class:

> All residents of the United States whose PII was compromised by Salesforce as a result of the Data Breach.

88. The Class excludes the following: Defendant, its affiliates, and its current and former employees, officers and directors, and the judge assigned to this case.

89. The Class definition may be modified, changed, or expanded based upon discovery and further investigation.

90. *Numerosity*: The Class is so numerous that joinder of all members is impracticable, evidenced by the large number of individuals presently known to have been injured by Defendant's conduct. The Class is ascertainable by records in the possession of Defendant or third parties.

[30] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement. (last visited Sept. 11, 2025)

91. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and Class members to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect PII as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class members' PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

j. Whether Plaintiff and Class members are entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

92. *Typicality*: Plaintiff's claims are typical of the claims of Class members. Plaintiff and Class members were injured and suffered damages in substantially the same manner, have the same claims against Defendant relating to the same course of conduct, and are entitled to relief under the same legal theories.

93. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Class and have no interests antagonistic to those of the Class. Plaintiff's counsel are experienced in the

prosecution of complex class actions, including actions with issues, claims, and defenses similar to the present case.

94. *Predominance and superiority*: Questions of law or fact common to Class members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all Class members is impracticable and the amount at issue for each Class member would not justify the cost of litigating individual claims. Should individual Class members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

95. Further, Defendant's unlawful conduct applies generally to all Class members, thereby making appropriate final equitable relief with respect to the Class as a whole.

V. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class)

96. Plaintiff realleges and incorporates by reference herein all preceding paragraphs as if fully set forth herein.

97. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and

probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

98. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Plaintiff and Class members entrusted their PII with Defendant, Defendant accepted and held the PII, and Defendant represented that the PII would be kept secure pursuant to its data security policies. Defendant could have ensured that its data security systems and practices were sufficient to prevent or minimize the Data Breach.

99. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

100. Defendant breached the aforementioned duties when it failed to use security practices that would protect Plaintiff's and Class members' PII, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

101. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

102. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

103. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the Breach.

104. The Breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

105. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, including but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

106. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

107. Neither Plaintiff nor the Class contributed to the Breach or subsequent misuse of their PII as described in this Complaint.

108. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have been put at an increased risk of credit fraud or identity theft, and Defendant must mitigate damages by providing adequate credit and identity monitoring services.

109. Plaintiff and Class members are entitled to damages for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year.

110. Plaintiff and Class members are entitled to damages to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and Class members have spent and will continue to spend

as a result of Defendant's negligence.

111. Plaintiff and Class members are entitled to damages to the extent their PII has been diminished in value because Plaintiff and Class members no longer control their PII and to whom it is disseminated.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

112. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

113. Defendant entered into various contracts with its clients, such as Transunion, to provide cloud-based software services to its clients.

114. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as Defendant agreed to safeguard and protect their confidential and private PII and to timely and accurately notify Plaintiff and Class Members if their information had been breached and compromised.

115. Defendant acquired, stored, and maintained the PII of Plaintiff and the Class.

116. Plaintiff and Class Members were required to provide, or authorize the transfer of, their PII in order for Defendant to provide its services and/or to receive services from a company (like Transunion) that uses Defendant's services.

117. Defendant solicited, offered, and invited Class Members to provide their private information as part of its regular business practices. Plaintiff and Class Members accepted Defendant's offer and provided their PII to Defendant and/or a company (like Transunion) that used Defendant's services.

118. When Plaintiff and Class Members provided their PII to Defendant (directly or indirectly), they entered into implied contracts with Defendant and intended and understood that PII would be adequately safeguarded as part of that service.

119. Defendant's implied promise of confidentiality to Plaintiff and Class Members includes consideration beyond those pre-existing general duties owed under the FTC Act, or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

120. Defendant's implied promises include but are not limited to: (a) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (b) restricting access to qualified and trained agents; (c) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (d) applying or requiring proper encryption; (e) multifactor authentication for access; (f) protecting Plaintiff's and Class Members' PII in compliance with federal and state laws and regulations and industry standards; and (g) other steps to protect against foreseeable data breaches.

121. Defendant's implied promises to safeguard Plaintiff's and Class Members' PII are evidenced by representations on Defendant's website. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is further demonstrated by their conduct and course of dealing.

122. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their PII to Defendant.

123. Defendant recognized that Plaintiff's and Class Members' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

124. Plaintiff and the Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

125. Defendant breached the implied contracts it made with its clients by failing to take reasonable measures to safeguard their PII as described herein, as well as by failing to

provide accurate, adequate, and timely notice to them that their PII was compromised as a result of the Data Breach.

126. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages from: (i) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (ii) the loss of the confidentiality of the stolen PII, (iii) the illegal sale of the compromised data on the dark web, (iv) lost work time, and (v) other economic and non-economic harms.

127. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to strengthen its data security systems, submit to future audits of those systems, and provide adequate long-term credit monitoring and identity theft protection services to all persons affected by the Data Breach.

COUNT III
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code §§1798.100, et seq.
(On Behalf of the Nationwide Class)

128. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

129. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA.

130. Plaintiff and Class Members are covered "consumers" under § 1798.140(g).

131. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

132. The PII of Plaintiff and Class members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the information Defendant collects and which was impacted by the Data Breach includes:

> [a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are 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.

Defendant collects, stores, or otherwise maintains consumers' PII.

133. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and Class Members' PII from unauthorized access, decryption, exfiltration, theft, and/or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

134. Defendant had and has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class Members' PII. As detailed herein, Defendant failed to do so.

135. As a direct and proximate result of Defendant's violation of its duty, some combination of Plaintiff's and Class Members' names with some combination of addresses and Social Security numbers, were subjected to unauthorized access and exfiltration, theft, or disclosure.

136. As a direct and proximate result of Defendant's acts, Plaintiff and the Class were injured and lost money or property, including, but not limited to, the loss of Plaintiff's and Class members' legally protected interest in the confidentiality and privacy of their PII, diminution of value of their PII, stress, fear, and anxiety, nominal damages, and additional losses described above.

137. Plaintiff has complied with the requirements of California Civil Code Section 1798.150(b), which provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." On September 17, 2025, Plaintiff provided Defendant with written notice identifying Defendant's violations of Cal. Civil

Code § 1798.150(a) and demanding the Data Breach be cured, pursuant to Cal. Civil Code § 1798.150(b).

COUNT IV
CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")
Cal. Civ. Code §§ 1798.80, et seq.
(On Behalf of the Nationwide Class)

138. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

139. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

140. The PII of Plaintiff and the Class at issue in this lawsuit constitutes "personal information" under § 1798.80(e), hereafter "PII."

141. Defendant is a business that owns, maintains, and licenses personal information within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiff and Class Members.

142. As alleged herein, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the unauthorized access, use and disclosure of Plaintiff's and Class Members' PII, in violation of § 1798.81.5(b).

143. Businesses that own or license computerized data that includes PII are required to notify California residents when their PII has been acquired, "or is reasonably believed to have been[] acquired by an unauthorized person" in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). Among other requirements, the security breach notification must include "the types of personal information

that were or are reasonably believed to have been the subject of the breach" pursuant to the model security breach form provided in Cal. Civ. Code § 1798.82(d).

144. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.80 and was thus subject to the disclosure requirements of Cal. Civ. Code § 1798.82.

145. Because Defendant reasonably believed that Plaintiff's and Class Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

146. Defendant has yet to directly inform Plaintiff and Class members of the Data Breach.

147. Defendant failed to fully disclose material information about the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

148. By failing to notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members were prevented from taking appropriate, reasonable precautions to mitigate harms caused by the Data Breach.

149. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and Class Members suffered damages, as described above.

150. Plaintiff and Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT V
CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code §§ 17200, et seq.
(On Behalf of the Nationwide Class)

151. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

152. The servers affected by the Data Breach were controlled and managed by Defendant and held all Plaintiff's and Class Members' PII.

153. Defendant meets the definition of a "person" as defined by Cal. Bus. & Prof. Code § 17201.

154. Plaintiff and Class Members each satisfy the definition of a "person" as defined by Cal. Bus. & Prof. Code § 17201.

155. Cal. Bus. & Prof. Code § 17204 provides that "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition" may file suit.

156. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

157. Defendant's "unfair" acts and practices include:

a. Failure to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' PII being compromised, and subsequent harms caused to Plaintiff and Class Members.

b. Failure to identify foreseeable security risks, including in their third-party vendor, Defendant, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

c. Failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; California's Consumer Privacy Act (Cal. Civ. Code § 1798.150); and HITECH Act, 42 U.S.C. § 17902;

d. Failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security practices and policies, consumers could not have reasonably avoided the harms that Defendant caused; and

e. With respect to Defendant, engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82 disclosure requirements.

158. Defendant engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); and HITECH Act, 42 U.S.C. § 17902.

159. Defendant engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); and HITECH Act, 42 U.S.C. § 17902.

160. Defendant engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); California's Consumer Privacy Act (Cal. Civ. Code § 1798.150); and HITECH Act, 42 U.S.C. § 17902.

161. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' PII being compromised, and subsequent harms caused to Plaintiff and Class Members;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach, unauthorized disclosure of Plaintiff's and Class Members' PII, and subsequent harms;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U. S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' PII being compromised, and subsequent harms caused to Plaintiff and Class Members;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150; and HITECH Act, 42 U.S.C. § 17902;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150; and HITECH Act, 42 U.S.C. § 17902.

162. Defendant's unfair and unlawful acts, e.g., failing to implement adequate security practices, harmed Plaintiff and Class members.

163. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Class members, about the adequacy of Defendant's data security policies and practices and ability to protect the confidentiality of consumers' PII.

164. Had Defendant disclosed to consumers that it was not complying with industry standards or regulations or that its data systems were not secure and, thus, were vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

165. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

166. Defendant was entrusted with sensitive and valuable PII regarding millions of consumers, including that of Plaintiff and Class Members. Defendant accepted the critical responsibility of protecting the PII but kept the inadequate state of its security controls secret from the public.

167. As a direct and proximate result of Defendant's unfair, unlawful, and/or fraudulent acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity and credit protection and repair services made necessary by the Data Breach.

168. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

169. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

170. By deceptively, unfairly, and unlawfully storing, collecting, and disclosing their PII, Defendant has taken money or property from Plaintiff and Class Members. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

171. Defendant was aware that the CRMs were a frequent target of sophisticated cyberattacks due to the recent increase in CRM attacks and high market value of PII, and on notice of the risks posed to consumers' PII that they collected, stored, used, and transferred in CRM's.

172. Defendant was on notice that its security and privacy policies and practices were wholly inadequate, including that of ensuring their vendors were compliant with industry standards and regulations, because of previous data breaches against CRM's.

173. Defendant knew or should have known that its data security was insufficient to guard against those attacks, particularly, given the size of its database and the sensitivity of the PII therein.

174. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VI
CALIFORNIA CONSTITUION'S RIGHT TO PRIVACY
Cal. Const., Art. I § I
(On Behalf of the Nationwide Class)

175. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

176. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

177. The right to privacy in California's Constitution creates a private right of action against private and government entities.

178. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

179. Defendant violated Plaintiff's and Class Members' constitutional right to privacy by collecting, storing, and disclosing, or preventing from unauthorized disclosure their PII in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy. Disclosure of their PII was highly offensive given the highly sensitive nature of the data. Accordingly, disclosure of Plaintiff's and Class Members' PII is an egregious violation of social norms.

180. Defendant intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential PII.

181. Plaintiff and Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of Defendant's lax and inadequate security practices with respect to securely collecting, storing, and using data, as well as preventing the unauthorized disclosure of consumers' PII; (ii) Plaintiff and Class Members did not consent or otherwise authorize Defendant to disclose their PII to parties responsible for the cyberattack; and (iii) Plaintiff and Class Members could not reasonably expect Defendant would commit acts in violation of laws protecting their privacy.

182. As a result of Defendant's actions, Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation.

183. Plaintiff and Class Members suffered actual and concrete injury as a result of Defendant's violations of their privacy interests. Plaintiff and Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

184. Plaintiff and Class Members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class Members' privacy.

COUNT VII
INJUNCTIVE/DECLARATORY RELIEF
(On Behalf of the Nationwide Class or, in the Alternative, the Class)

185. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

186. Defendant owes a duty of care to Plaintiff and Class members requiring it to adequately secure PII.

187. Defendant still stores Plaintiff's and Class members' PII.

188. Since the Data Breach, Defendant has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

189. Defendant has not satisfied its legal duties to Plaintiff and Class members.

190. Actual harm has arisen in the wake of the Data Breach regarding Defendant's duties of care to provide security measures to Plaintiff and Class members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their PII, and Defendant's failure to address the security failings that led to that exposure.

191. Plaintiff, therefore, seeks a declaration: (a) that Defendant's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

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

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

d. ordering that Defendant segment customer PII by, among other things, creating firewalls and access controls so that if one area of Defendant's

system is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. ordering that Defendant purge, delete, and destroy in a reasonably secure manner PII not necessary for its provision of services;

f. ordering that Defendant conduct regular computer system scanning and security checks; 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

g. ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face because of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment as follows:

a. For an order certifying the Class, appointing Plaintiff as Class Representative, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory, punitive, statutory, and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees; and

f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff hereby respectfully demands a trial by jury.

Dated: September 19, 2025

Respectfully submitted,

/s/Colleen L. Fewer

Colleen L. Fewer (SBN 323808)
BERGER MONTAGUE PC
505 Montgomery Street, Suite 625

San Francisco, CA 94111
T. 415.376.2097
F.215.875.4604

E. Michelle Drake (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
T. 612.594.5999
F. 612.584.4470
emdrake@bm.net

Mark B. DeSanto (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
T. 215.875.3000
F. 215.875.4604
mdesanto@bm.net

Counsel for Plaintiff and Proposed Class