Danielle L. Perry (CA Bar No. 292120)
MASON & PERRY LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

Counsel for Plaintiff and the Proposed Class

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JENNI SUHR, individually and on behalf of all others similarly situated,

Plaintiff,

v.

WOFLOW INC.,

Defendant.

Case No.: 3:26-cv-02161

CLASS ACTION COMPLAINT:

1. Negligence
2. Invasion of Privacy – Public Disclosure of Private Facts, and California Constitutional Right to Privacy
3. Violation of California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*
4. Violation of California Consumer Privacy Act, Cal. Civ. Code §§ 1798.80, *et seq.*

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jenni Suhr ("Plaintiff"), individually and on behalf of all persons who are similarly situated, brings this action against Defendant Woflow Inc. ("Woflow" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant Woflow on or around early March 2026[1] (the "Data Breach"), which held in its possession certain personally identifiable information ("PII" or "the Private Information") of Plaintiff and other individuals, the putative Class Members ("Class"), who were associated with Defendant Woflow. These individuals, upon information and belief, include consumers who engaged in services provided by Woflow and employees with Woflow.

2. The private information involved in the data breach included personal data information, including, but not limited to: full names, addresses, Social Security numbers, driver's license numbers, financial account details, and other credit card account details.

3. Upon information and belief, the Private Information was compromised in a cyberattack on Woflow's inadequately protected computer network. In other words, the cybercriminals intentionally targeted Woflow for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then had unfettered access to Defendant's computer network,

[1] https://www.redpacketsecurity.com/shinyhunters-ransomware-victim-woflow-inc/ (last visited March 12, 2026).

exfiltrating highly sensitive PII, including Social Security numbers. As a result, the Private Information of Plaintiff and the Class remains in the hands of those cybercriminals.[2]

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for purchases and employment.

5. Plaintiff brings this class action lawsuit on behalf of herself and all persons who are similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, for failing to promptly detect the cyberattack, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access and exfiltration by cybercriminals.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Woflow's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant disregarded the rights of Plaintiff and Class Members by, inter alia, intentionally, willfully, recklessly, 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' Private Information; failing to take standard and reasonably available steps to

[2] *Id.* (last visited March 12, 2026).

prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

8. In addition, Defendant Woflow failed to properly monitor the computer network and systems that housed the Private Information. Had Woflow properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals unimpeded access to the PII of Plaintiff and Class Members for an undisclosed amount of time.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant Woflow collected and maintained is now in the hands of cybercriminals, and their Private Information has been posted, sold or is in imminent risk of being sold on the Dark Web.

10. Armed with the Private Information accessed in the Data Breach, cybercriminals can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members have or soon may incur out-of-pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

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

14. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) Invasion of Privacy – Public Disclosure of Private Facts, and California Constitutional Right to Privacy, (iii) violation of California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*.; and (iv) violation of California Consumer Privacy Act, Cal. Civ. Code §§ 1798.80, *et seq*.

15. 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.

PARTIES

16. Plaintiff Jenni Suhr is and at all times mentioned herein was an individual citizen of the State of Colorado. Ms. Suhr receives Woflow services.

17. Defendant Woflow Inc. is a technology corporation formed in California, with its principal place of business located at 45 Belden Place, Suite 300, San Francisco, California 94104. Woflow can be served by its registered agent, Jordan Nemrow, at its principal place of business.

JURISDICTION AND VENUE

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

19. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a stock corporation; it maintains its headquarters in California; and committed tortious acts in California.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Woflow has the most significant contacts.

FACTUAL ALLEGATIONS

Defendant's Business

21. Woflow is a technology company that provides artificial intelligence ("AI") tools and services designed to support business operations, including software that allows organizations to build, train, and deploy AI-driven agents.[3]

22. Woflow offers an artificial intelligence platform used by enterprise organizations to build, train, and deploy AI agents within their business operations. Through this platform, Woflow enables companies to automate workflows and perform operational tasks using AI-driven systems."[4]

23. As described on its website, Woflow provides tools and services that allow organizations to evaluate AI systems, monitor performance, train AI agents using real-world data and feedback, and integrate those agents into existing operational systems and software environments.[5]

24. In providing these services, Woflow processes and interacts with business information and operational data belonging to its customers and their users in order to support automated workflows and AI-driven tasks within client organizations.

[3] https://www.woflow.com/#use-cases-section (last visited March 12, 2026).
[4] https://www.woflow.com/#platform-section (last visited March 12, 2026).
[5] *Id.*

25. In the ordinary course of providing its platform and services, Woflow integrates with and operates within its customers' and/or third-party systems and applications, which store and process sensitive personal information. As a result, Woflow's services access, process, store, and/or interact with personally identifiable information ("PII") belonging to customers and end users whose data is maintained within those systems, including but not limited to:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Demographic information;
- Financial Account information; and
- Driver's license or state or federal identification.

26. Upon information and belief, Woflow has a privacy policy that is provided upon accepting services.[6]

27. Defendant represents in its Privacy Policy that it maintains security measures to protect personal information, stating: "We have organizational and technical processes and procedures in place to protect your personal information." By collecting, storing, processing, and interacting with sensitive personally identifiable information through its platform and integrations with customer systems, Defendant represented that it would implement and maintain reasonable security measures designed to safeguard that information from unauthorized access, disclosure, or misuse."[7]

28. Defendant Woflow agreed to and undertook legal duties to maintain the protected personal information entrusted to it by by customers for and on behalf of Plaintiff and Class Members, and it promised to do so safely, confidentially, and in

[6] https://www.woflow.com/legal/privacy-policy (last visited March 12, 2026).
[7] *Id.*

compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45 and the California Online Privacy Protection Act.

29. Yet, through its failure to properly secure the Private Information of Plaintiff and the Class, Woflow has not adhered to its own promises of individuals' rights.[8]

30. The Private Information held by Defendant Woflow in its computer system and network included the highly sensitive Private Information of Plaintiff and Class Members.

The Data Breach

31. A Data Breach occurs when cybercriminals gain unauthorized access to and steal private information that has not been adequately safeguarded by a business entity, such as Woflow.

32. Upon information and belief, Defendant experienced a cyberattack on its computer systems by threat actor Shinyhunters on or before March 3, 2026, when it took many of the business's networked systems offline, adversely affecting its platform services.[9]

33. As of the filing of this Complaint, upon information and belief, the required State Attorney Generals' notices have not been sent, nor have consumers and employees received direct notice of whether their Private Information was breached and exfiltrated.

34. Upon information and belief, Shinyhunters has disseminated the PII of consumers and employees taken from Woflow's ineadequately protected computer systems on the Dark Web.

[8] *Id.*

[9] https://www.redpacketsecurity.com/shinyhunters-ransomware-victim-woflow-inc/ (last visited March 12, 2026).

35. ShinyHunters is a criminal hacker and extortion group that is believed to have formed in 2019, and is said to have been involved in a massive number of significant data breaches. Using a "pay or leak" model, they often extort the company they've hacked, if the company does not pay the ransom the stolen information is leaked or sold on the dark web.

36. In its 2025 Financial Trend Analysis, FinCEN reported that ransomware remains a significant and well-documented threat to the business and financial sectors, with ransomware payments surging 77% to 1.1 billion dollars in 2023 and staying elevated through 2024. The report, based on recent Bank Secrecy Act filings, shows that financial-services organizations alone accounted for roughly 365.6 million dollars in payouts between 2022 and 2024 and were among the top three most-targeted industries in that period. These recent data points demonstrate that, in the contemporary business and financial environment, the risk of ransomware attacks is closely tracked, quantified, and therefore both foreseeable and addressable through robust cybersecurity and compliance programs.[10]

37. Woflow's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

38. Woflow knew or should have known that its electronic records would be targeted by cybercriminals.

39. Woflow has failed to publicly disclose crucial details regarding the data security incident, including when the breach occurred, how long unauthorized access persisted, and other pertinent facts. This lack of transparency has deprived Plaintiff and Class Members of information needed to protect themselves from potential harm, such as identity theft and fraud, and to take meaningful steps to mitigate further damages.

---

[10] https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware (last visited March 12, 2026).

40. Upon information and belief, Woflow has not provided complimentary credit monitoring or identity theft protection services to Plaintiff and Class Members whose sensitive personal information was exposed in the Data Breach.

41. Defendant had obligations created by the California statutes, FTCA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

42. Plaintiff and Class Members provided their Private Information to Defendant and Defendant's customers with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach Was a

Foreseeable Risk of Which Defendant Was on Notice.

43. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cybercriminals. Organizations that collect such information, including Woflow, are well-aware of the risk of being targeted by cybercriminals.

44. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

45. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that

were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[11]

46. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

47. Data breach victims suffer long-term consequences when their PII and Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

48. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[12]

49. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[13]

---

[11] "Victims of Identity Theft, 2018," U.S. Dep't of Justice (Apr. 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited March 12, 2026).

[12] https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited March 12, 2026).

[13] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in -2021-new-report-says/ (last visited March 12, 2026).

50. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[14]

51. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

52. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[15] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[16]

53. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private

[14] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited March 12, 2026).

[15] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited March 12, 2026).

[16] *Id.*

and secure, Woflow failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

Defendant Fails to Comply with FTC Guidelines.

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

55. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

56. The FTC further recommends that organizations not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[17] *Protecting Personal Information: A Guide for Business*, FTC (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-informatio n.pdf (last visited March 12, 2026).

[18] *Id.*

57. The FTC has brought enforcement actions against organizations like Woflow's for failing to adequately and reasonably protect individuals' data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Defendant failed to properly implement basic data security practices.

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

60. Defendant was at all times fully aware of its obligation to protect the Private Information of individuals seeking or receiving services. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards.

61. As shown above, experts studying cybersecurity routinely identify software and management service providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

62. Several best practices have been identified that a minimum should be implemented by service providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the service industry include installing appropriate malware detection software; monitoring and

limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

64. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

65. These frameworks are existing and applicable industry standards, yet Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant Has Breached its Obligations to Plaintiff and the Class.

66. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Woflow's computer systems and Class Members' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Class Members' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to promptly prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic data;

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules regarding individually identifiable information;

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PII as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PII; and/or

m. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals.

67. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees

who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

68. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identity Theft.

69. Data Breaches such as the one experienced by Woflow are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

70. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[19] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit A. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and the Class) must take after a breach like Woflow's are both time consuming and of only limited and short term effectiveness.

71. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[20]

[19] https://www.gao.gov/assets/gao-19-230.pdf (last visited March 12, 2026). *See* attached as Ex. A.

[20] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Gov't Acct. Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited March 12, 2026). ("2007 GAO Report").

72. The FTC, like the GAO (*see* Exhibit A), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

73. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

74. Identity thieves can also use Social Security numbers to 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 Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

75. Theft of Private Information is also gravely serious. Private Information is a valuable property right.[22]

76. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

[21] *See* https://www.identitytheft.gov/Steps (last visited March 12, 2026).

[22] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

77. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

78. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their personal, financial, and medical accounts for many years to come.

79. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[23] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[24] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the

[23] *Identity Theft and Your Social Security Number* at 1, Soc. Sec. Admin. (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited March 12, 2026).
[24] *Id.* at 4.

individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

80. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link 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."[25]

81. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[26]

82. Stolen PII is often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals. The record sets are then sold on dark web sites to other criminals and allow individual identity kits to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities.[27]

---

[25] Brian 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-millions-worrying-about-identity-theft (last visited March 12, 2026).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited March 12, 2026).

[27] *See* https://www.fraud.net/glossary/fullz#what-is-fullz (last accessed March 12, 2026).

83. In recent years, service and management industries have experienced higher numbers of data theft events. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S EXPERIENCE

Plaintiff Jenni Suhr

84. Plaintiff Jenni Suhr is and at all times mentioned herein was an individual citizen residing in the State of Colorado.

85. Plaintiff Suhr is a consumer who utilizes Woflow's services. Plaintiff provided Woflow with her full name, date of birth, phone number, and address, as well as other financial information required on Woflow's platforms.

86. Upon information and belief, this Private Information was maintained on Woflow's computer systems on or around the time of the Data Breach, when those systems were subject to unauthorized access and exfiltration by cybercriminals, ShinyHunters. Plaintiff's Private Information, therefore, was among the data compromised in the incident.

87. Following the Data Breach, Plaintiff independently became aware of the incident while conducting her own online research, prompted by a marked increase in spam notifications, which is a recognized indicator of unauthorized access to personal information commonly associated with data breaches.

88. Plaintiff reasonably believes that her Private Information was sold on the Dark Web as a part of this Data Breach. As a result of this breach, Plaintiff has taken efforts to mitigate the impacts of identity theft and fraud by closely monitoring her accounts, continuing to research the breach, changing her passwords, and contacting an attorney for help.

89. For a little while now, Plaintiff has been receiving a combination of around 5-10 spam calls, texts, and many spam emails per day. Prior to this time, she was receiving maybe one troublesome call and/or email per day.

90. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a social engineering attack.

91. Since the Data Breach, Plaintiff monitors her financial accounts for about one to two hours per week. This is more time than she spent prior to learning of Woflow's Data Breach. Having to do this every week not only wastes his time due to Woflow's negligence, but also causes her great concern.

92. Plaintiff is alarmed and very concerned that her Private Information is in the hands of cybercriminals. She is aware that cybercriminals often sell Private Information, and that this could be abused months or even years after this Data Breach.

93. Had Plaintiff been aware that Woflow's computer systems were not secure, she would not have entrusted Woflow with her Private Information.

PLAINTIFF'S AND CLASS MEMBERS' INJURIES

94. To date, Defendant Woflow has done absolutely nothing to compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

95. Defendant Woflow has yet to offer credit monitoring services to victims, a tacit admission that its failure to protect their Private Information has caused Plaintiff and the Class great injuries. This lack of care is inadequate when victims are likely to face many years of identity theft.

96. Woflow fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff's

and Class Members' Private Information, out-of-pocket costs, and the time they are required to spend attempting to mitigate their injuries.

97. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

98. Plaintiff's and Class Members' Private Information was compromised and exfiltrated by cybercriminals as a direct and proximate result of the Data Breach.

99. Plaintiff and Class Members were damaged in that their Private Information is now in the hands of cybercriminals, sold and potentially for sale for years into the future.

100. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

101. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

102. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members have or may in the near future incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

103. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

104. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

105. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

106. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

107. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

108. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

109. Defendant's delay in identifying and reporting the Data Breach caused additional harm. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft.

CLASS ACTION ALLEGATIONS

110. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

111. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach experienced by Woflow Inc. in March 2026 (the "Class").

112. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

113. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

114. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Upon information and belief the number of Class Members consists of thousands of individuals.

115. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

116. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

117. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

118. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

119. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

120. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

121. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

122. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count

Negligence

(On Behalf of Plaintiff and Class Members)

123. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

124. Defendant Woflow required Plaintiff and Class Members to submit (through its business customers, connected applications, or otherwise) non-public personal information in order to access, use, or interact with services supported by Woflow's platform.

125. By collecting and storing this data in Woflow's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

126. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

127. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission 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 confidential data.

128. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

129. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

130. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

131. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

132. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

133. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

134. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Second Count

Intrusion Upon Seclusion / Invasion of Privacy

(On Behalf of Plaintiff and All Class Members)

135. Plaintiff and incorporates by reference each and every material fact of this Complaint as if fully set forth herein.

136. The State of California recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the RESTATEMENT (SECOND) OF TORTS, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

RESTATEMENT (SECOND) OF TORTS § 652B (1977).

137. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

138. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

139. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

140. Defendant knew that an ordinary person in Plaintiff's or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

141. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

142. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

143. The conduct described above was at or directed at Plaintiff and the Class Members.

144. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would

consider Defendant's intentional actions or inaction highly offensive and objectionable.

145. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seek an award of damages and injunctive relief on behalf of themselves and the Class.

Third Count

Violation of the California Unfair Competition Law

Cal. Bus. & Prof Code §§ 17200, *et seq.* – Unlawful Business Practices

(On Behalf of Plaintiff and All Class Members)

146. Plaintiff realleges and incorporates by reference each and every material fact of this Complaint as if fully set forth herein..

147. Defendant has violated Cal. Bus. and Prof. Code §§ 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

148. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' Private Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding the Private Information of Plaintiff and the Class Members.

149. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 and Cal. Health & Safety Code § 1280.15(b)(2).

150. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

151. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

152. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code §§ 17200, *et seq*., including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Fourth Count

Violation of California Consumer Privacy Act ("CCPA")

Cal. Civ. Code §§ 1798.80, *et seq.*

(On Behalf of Plaintiff and Class Members)

153. Plaintiff realleges and incorporates by reference each and every material fact of this Complaint as if fully set forth herein..

154. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . .."

155. The CCPA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

156. The Data Breach described above constituted a "breach of the security system" of Defendant, within the meaning of Civil Code § 1798.82(g).

157. The information lost in the data breach constituted "personal information" within the meaning of Civil Code § 1798.80(e).

158. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Breach.

159. Defendant unreasonably delayed informing anyone about the Breach after Defendant knew the Breach had occurred. Defendant waited nearly three months after becoming aware that attackers had gained access to Plaintiff's and

Class Members' PII before beginning the process of notifying individuals of the Breach.

160. Defendant failed to disclose to Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when they knew or reasonably believed such information had been compromised.

161. Upon information and belief, no law enforcement agency instructed Defendant that notification to Class Members would impede investigation.

162. As a result of Defendant's violation of Civil Code §§ 1798.80, *et seq.*, Plaintiff and other Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

163. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their stolen information would have had less value to identity thieves.

164. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

165. Plaintiff and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and Class Members as alleged above and equitable relief.

166. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff and Class Members of "legal rights or otherwise causing injury." In addition,

Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and Class Members and despicable conduct that has subjected Plaintiff and Class Members to hardship in conscious disregard of their rights. As a result, Plaintiff and Class Members are entitled to punitive damages against Defendant under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: March 12, 2026

Respectfully submitted,

/s/ Danielle L. Perry

Danielle Perry (SBN 292120)
MASON & PERRY LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

Attorney for Plaintiff

EXHIBIT A

Appendix II: What Can Consumers Do After a Data Breach?

Figure 3 below provides information on actions consumers can take to monitor for identity theft or other forms of fraud, protect their personal information, and respond if they have been a victim of identity theft. This information summarizes prior GAO work and comments of academic, consumer organization, industry, and government experts.[1]

[1]GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C.: Mar. 30, 2017).

Figure 3: What Can Consumers Do After a Data Breach?

Prevent Fraud on New Credit Accounts

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Place a credit freeze** on credit reports at Equifax, Experian, and TransUnion—the three nationwide consumer reporting agencies.	• Prevents identity thieves from opening new credit accounts in an individual's name—where credit reports are required. • Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated.	• Consumers must request a freeze at each of the three agencies separately. • Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports. • Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card). • Freezes do not prevent other types of harm, such as tax refund or medical identity fraud. • Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks). • Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts).
 **Place a fraud alert** at the three nationwide consumer reporting agencies, which lasts 1 year and can be renewed.	• Fraud alerts let businesses know that a consumer may have been a victim of fraud. • Businesses must take extra steps to verify the identity of the individual seeking to open accounts. • Members of the military can place active duty alerts.	• Consumers can request a fraud alert at one of the three agencies and this agency must notify the other two to place the alert. • Victims of identity theft can place extended fraud alerts that last for 7 years. • Fraud alerts still allow access to credit reports. • Businesses that do not use the three agencies will not see the alert.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Some Types of Fraud on Financial Accounts

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Review free credit reports every 12 months** (from Equifax, Experian, and TransUnion) at annualcreditreport.com.	• Can help consumers spot suspicious activity or fraud involving credit accounts.	• Consumers can check one of the three reports every 4 months to improve chances of catching problems throughout the year.
 **Review bank and other financial account statements regularly or set up free automatic alerts.**	• Can alert consumers to suspicious activity on their accounts.	• The availability and features of alerts may vary among financial institutions.
 **Consider enrolling in credit or identity monitoring services.**	• Credit monitoring can alert consumers after the fact that someone may have used their personal information to open a credit account (take out a loan or sign up for a credit card). • Identity monitoring can alert consumers of misuse of personal information or appearance of their information on illicit websites (the “dark web”).	• These services do not directly address risks of medical identity theft, identity theft tax refund fraud, or government benefits fraud. • Credit monitoring can spot fraud but generally cannot prevent it, and does not identify fraud on existing or noncredit accounts. • Identity monitoring also cannot prevent fraud. • It is unclear what actions consumers can take once alerted that their information appears on the dark web other than continuing to monitor their accounts. • These services may be part of a package of identity theft services, including restoration services, or identity theft insurance. • Free services that entities that have experienced data breaches may offer to affected consumers vary in the type and level of service and may only last for 1-2 years. Risks can exist for much longer. • Paid services typically cost $5–$30 a month.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Other Types of Identity Theft or Fraud

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Mobile Phone or Utility Account Fraud**		
Review mobile phone and utility bills regularly.	• Can spot suspicious activity on existing accounts.	• Consumers with credit freezes may need to lift them before applying for new utility or phone accounts.
 **Medical Identity Theft**		
Review medical bills and health insurance explanations of benefits.	• Can spot suspicious activity, such as bills or insurance claims for services consumers did not receive.	• Consumers who spot problems can contact fraud departments at health insurers.
 **Identity Theft Tax Refund Fraud**		
File tax returns early.	• Provides less time for a fraudster to file in an individual's name.	• Consumers who experience identity theft tax refund fraud can file affidavits with the Internal Revenue Service (IRS) and through IdentityTheft.gov, and may be eligible to obtain an Identity Protection Personal Identification Number from IRS.
 **Government Benefits Fraud**		
Set up an online account at the Social Security Administration and check it regularly.	• Can spot suspicious activity, such as benefits redirected to another address.	• Other government benefits, such as unemployment insurance, also can be susceptible to identity fraud.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

How to Respond after Identity Theft		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
Visit identityTheft.gov to set up an account, fill out, and file necessary reports.	• Helps users determine what steps to take depending on the type of information stolen or type of identity theft. • Can generate an Identity Theft Report that can be used to help contact consumer reporting agencies, law enforcement, and other entities. • Can generate an IRS Identity Theft Affidavit (IRS Form 14039) that can be submitted directly to IRS. • Provides information on what companies to contact and how to remove incorrect information.	• The Federal Trade Commission (FTC) also has a telephone help line and online chat feature.
Contact state or local government resources, such as consumer protection help lines or victim services offices.	• Some states and local governments can provide one-on-one assistance.	• States and localities vary in the services offered.
Consider using commercial identity restoration services.	• Can reduce consumer time and effort in dealing with the effects of identity theft, such as by interacting with creditors on the consumer's behalf.	• Service levels can vary significantly among companies. Some provide hands-on assistance, while others largely provide information. • May be included in a package of identity theft services, which may also include credit or identity monitoring or identity theft insurance. Paid services typically cost $5–$30 a month and free services may only be offered for 1-2 years.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Protect Personal Information in Other Ways

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Adopt Good Practices for Online Accounts** • Protect passwords and do not re-use them. • Use two-factor authentication when offered (for example, entering a one-time code sent to a mobile phone when logging in to an online account). • Choose strong passwords and consider using a software application that helps manage passwords. • Do not click on links in emails or open attachments from unknown senders. • Remember that public WiFi may not be secure.	• Can prevent unauthorized access to online accounts and other data intrusions.	• While personal security practices are important, consumers have limited control over how private entities secure their data.
 **Protect social media accounts** by checking privacy settings, and consider limiting information shared.	• Restricts how much information is visible to strangers and their ability to misuse it.	• Privacy terms and conditions can change, so it is important to check settings periodically.
 **Do not provide personal information over the phone (or by email or text) unless you've initiated the call (or communication).**	• Prevents identity thieves from obtaining information that can be used to commit fraud.	• Consumers can do online searches to verify identities of requesters, or check with experts, before giving out information. • Consumers should not trust caller ID and should hang up on robocalls and report such calls to FTC at ftc.gov/complaint.
 **Shred documents and mail with Social Security numbers or other personal information.**	• Prevents identity thieves from finding sensitive information in trash.	• Consumers can contact the U.S. Postal Service if they believe their mail is being stolen or misdirected. • Consumers can opt out of receiving credit card and other offers in the mail at 1-888-5-OPT-OUT (1-888-567-8688) or www.optoutprescreen.com.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230