Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Jeff S. Westerman (SBN 94559)
jwesterman@ahdootwolfson.com
Lisa M. Cintron (SBN 356009)
lcintron@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
Tel: 310-474-9111
Fax: 310-474-8585

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL WALSH, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CHIME FINANCIAL, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Michael Walsh ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendant Chime Financial, Inc. ("Chime" or "Defendant"):

INTRODUCTION

1. Plaintiff brings this class action individually and on behalf of all other individuals who had their sensitive personal information, including but not limited to: names, Social Security numbers (SSN), dates of birth, postal and email addresses, phone numbers, government-issued IDs, financial and credit-related information, account credentials, employment information, biometric data, precise geolocation data, and other personally identifiable information (collectively, "PII" or "Personal Information") disclosed to unauthorized third parties during a data breach compromising Chime in or around April 2026 (the "Data Breach").

2. Defendant Chime is a financial technology company that provides digital banking services to millions of consumers across the United States.[1]

3. On or about April 1, 2026, Chime experienced a widespread service outage that prevented users from accessing their accounts, including logging in, checking balances, initiating transactions, or using key features of the Chime platform.[2] Contemporaneous outage data confirmed that the disruption was widespread and systematic, with more than 20,000 user reports at its peak.[3]

4. At or about the same time, Defendant acknowledged the incident on its official system status page, stating: "We're currently investigating a service disruption across our platform. We're working hard to resolve this issue as soon as possible. Card purchases and ATM transactions are working normally. The money in your account and your personal information are secure."[4]

---

[1] Chime Fin., Inc., *About Us*, https://www.chime.com/about-us/.

[2] *See Is Chime Down? What Users Should Know*, Newsweek (Apr. 1, 2026), https://www.newsweek.com/chime-down-outage-service-status-not-working-11770861.

[3] *Id.*

[4] *See Chime is Down Today And Here Is What Is Working And What Is Not*, Artvoice (Apr. 1, 2026), https://artvoice.com/2026/04/01/chime-is-down-today-and-here-is-what-is-working-and-what-is-not/.

5. Defendant did not disclose what caused the outage, but public reports indicate that the outage stemmed from a coordinated cyberattack targeting Defendant's systems.[5]

6. A threat actor group known as "Team 313" claimed that it had conducted a "massive cyberattack targeting the servers of Chime," which caused the company's systems to crash and completely disabled the application and website."[6] Team 313 further asserted that, in addition to causing operational disruption, it exfiltrated sensitive customer data, including personally identifiable information ("PII") from Defendant's systems, and intended to publish such data on the dark web.[7]

7. Despite the scale of the outage, the nature of the attack, and the threat actor's claims of data exfiltration, Defendant has not provided formal notice to affected users confirming whether their PII was compromised.

8. Defendant was well aware of or should have known of its data security shortcomings. Chime routinely collects and maintains extensive Personal Information from customers and prospective customers through its websites, mobile applications, bank partners, vendors, and payment processors. Nevertheless, Chime failed to implement industry standard data privacy measures, exposing its customers and other affiliated individuals to the risk of being impacted by a breach.

9. Defendant's failures to ensure that its servers and systems were adequately secure jeopardized the security of Plaintiff's and Class Members' Personal Information, and exposed Plaintiff and Class Members to fraud and identity theft or the serious risk of fraud and identity theft.

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

---

[5] *Chime Goes Down for Thousands of Users,* GV Wire (Apr. 1, 2026), https://gvwire.com/2026/04/01/chime-goes-down-for-thousands-of-users-downdetector-shows/.

[6] *See* Margi Murphy & Page Smith, *Pro-Iran Group Takes Credit for Cyberattacks on Chime, Pinterest,* Bloomberg Government (Apr. 7, 2026), https://news.bgov.com/bloomberg-government-news/pro-iran-group-takes-credit-for-cyberattacks-on-chime-pinterest.

[7] *Id.*

PARTIES

Plaintiff

11. Plaintiff Michael Walsh is an adult citizen of the state of California and resides in Los Angeles County, California. Plaintiff is a customer of Chime. Believing Chime would implement and maintain reasonable security practices to protect customer Personal Information, Plaintiff provided his sensitive Personal Information to Defendant in connection with seeking financial products and services from Chime.

12. On information and belief, Chime did not take proper care of Plaintiff's Personal Information. Plaintiff recently received an alert from his bank indicating that an unauthorized charge was attempted on his credit card. Additionally, he has been informed that his Personal Information has been discovered on the dark web. To date, Plaintiff has spent several hours checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff will need to continue indefinitely to protect against fraud and identity theft.

13. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Defendant

14. Defendant Chime Financial, Inc. is a corporation organized under the laws of the state of Delaware with its principal place of business at 101 California Street, Suite 500, San Francisco, CA 94111.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class members, the action is a class action in which one or more Class members are citizens of states different from Defendant, and Defendant is not a government entity.

16. The Court has personal jurisdiction over Defendant because Defendant has a principal office in San Francisco, California, operates in California, conducts other significant business in

California, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in California.

17. Venue properly lies in this judicial district because, inter alia, Defendant has a principal place of business in this district; Defendant transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Defendant Collects and Stores Personal Information

18. Chime is a financial technology company that provides digital banking services to millions of consumers across the United States.[8]

19. In the ordinary course of its business, Defendant collects, stores, and maintains vast quantities of highly sensitive PII and financial information from its customers and prospective customers.

20. Defendant's own U.S. Privacy Notice confirms that it collects broad categories of personal information and represents that it takes measures to protect such data, stating:

> This Privacy Notice ("Notice") describes the types of personal information we collect, how we use the information, with whom we may share it, and the choices available to you. We also describe measures we take to protect the security of the information and how you can contact us about our privacy practices.[9]

21. According to Defendant's Privacy Notice, the categories of personal information it collects includes:

- Identifiers, such as names, Social Security numbers, dates of birth, postal and email addresses, and phone numbers;
- Government-issued identification, such as driver's licenses, passports, and identity verification documents;
- Account credentials, including usernames and passwords;
- Financial information, including account numbers, transaction history, linked account data, and payment card information;

[8] Chime Fin., Inc., *About Us*, https://www.chime.com/about-us/.

[9] Chime Fin., Inc., *U.S. Privacy Notice*, https://www.chime.com/policies/chime/privacy-policy/ (the "Chime Privacy Notice").

- Employment and income information, including employer details and compensation data;
- Credit and tax-related information, including credit history and tax return data;
- Biometric and identity verification data, including photographs and derived biometric identifiers; and
- Other sensitive personal information, including precise geolocation data and demographic information.[10]

22. Defendant also collects a wide range of additional data, including commercial information, voice recordings, social media identifiers, lease and rental information, and inferences derived from consumer behavior and usage patterns, further expanding the scope and sensitivity of the data it maintains.[11]

23. Defendant expressly represents that it employs robust security measures to protect Personal Information:[12]

> **Does Chime protect my data?**
> The security of your personal data is as important to Chime as the security of your money.
> …
>
> **Encryption and secure transmission**
> All personal data needed to open a Chime account, including your name, address, birth date, and Social Security number, is protected by at least 128-bit encryption both during transit and at rest.
>
> Whether you're checking your account balance, paying bills, or sending money to a friend, your data is secure in the Chime app.
>
> **Privacy-first design**
> At Chime, we know that your privacy is of utmost importance. That's why we keep your personal information private. We never sell our members' data for marketing purposes, so you don't need to worry about getting spam calls, texts, and emails.

[10] *See* Chime Fin., Inc., *U.S. Privacy Notice—Information We Obtain*, https://www.chime.com/policies/chime/privacy-policy/#information-we-obtain.

[11] *See Chime Privacy Notice—Information We Obtain*, *supra.*

[12] Chime Fin., Inc., *Is Chime Safe? What You Need to Know* (Jan. 13, 2026), https://www.chime.com/blog/is-chime-safe/.

24. Defendant further represents that it maintains "administrative, technical and physical safeguards designed to protect the personal information [customers] provide against accidental, unlawful or unauthorized access, destruction, loss, alteration, disclosure or use."[13]

25. Defendant's public facing privacy materials make clear that Defendant was aware of the need to safeguard the sensitive Personal Information entrusted to it, and of the potentially severe consequences that follow when such sensitive Personal Information is not adequately secured.

B. The Data Breach

26. On or about April 1, 2026, Chime experienced a widespread service outage that prevented users across the United States from accessing their accounts, including logging in, checking balances, initiating transactions, or using key features of the Chime platform.[14]

27. Public reports suggest that the outage was not caused by a routine technical failure, but rather by a coordinated cyberattack targeting Defendant's systems, resulting in a system-wide disruption.[15] At the peak of the incident, tens of thousands of users reported issues accessing the platform, with some estimates suggesting that approximately 20,000 users were affected.[16]

28. A threat actor group known as "Team 313" publicly claimed responsibility for the attack, asserting that it had infiltrated Defendant's systems and launched a coordinated attack targeting its servers.[17]

29. Team 313, also referred to in threat intelligence reporting as "Cyber Islamic Resistance (Team 313)" is an identified cyber threat actor operating within a broader ecosystem of pro-Iranian

---

[13] *See* Chime Fin., Inc., *U.S. Privacy Notice—How We Protect Personal Information*, https://www.chime.com/policies/chime/privacy-policy/#how-we-protect-personal-information.

[14] *See, e.g., Chime is Down Today And Here Is What Is Working And What Is Not*, Artvoice (Apr. 1, 2026), https://artvoice.com/2026/04/01/chime-is-down-today-and-here-is-what-is-working-and-what-is-not/; *Is Chime Down? What Users Should Know*, Newsweek (Apr. 1, 2026), https://www.newsweek.com/chime-down-outage-service-status-not-working-11770861.

[15] *Chime Goes Down for Thousands of Users,* GV Wire (Apr. 1, 2026), https://gvwire.com/2026/04/01/chime-goes-down-for-thousands-of-users-downdetector-shows/.

[16] *See id.*

[17] *See* Margi Murphy & Page Smith, *Pro-Iran Group Takes Credit for Cyberattacks on Chime, Pinterest,* Bloomberg Government (Apr. 7, 2026), https://news.bgov.com/bloomberg-government-news/pro-iran-group-takes-credit-for-cyberattacks-on-chime-pinterest.

hacktivist and proxy groups engaged in coordinated cyber campaigns against commercial and governmental targets.[18] Team 313 employs a structured operational model characterized by a "disrupt, leak, and amplify" strategy, in which attackers pair service outages with claims of data exfiltration and public dissemination of stolen information.[19]

30. Consistent with this pattern, Team 313 claimed that it had conducted a "massive cyberattack" that caused Defendant's systems to crash, while also asserting that it exfiltrated sensitive customer data, including personally identifiable information, and intended to publish such data on the dark web.[20]

31. Team 313's claims regarding the unauthorized acquisition and threats to disclose that data are sufficiently credible based on the threat actor's known modus operandi.

32. Upon information and belief, the information accessed and exfiltrated as a result of the Data Breach includes, but is not limited to, Plaintiff's and Class Members' names, Social Security numbers (SSN), dates of birth, postal and email addresses, phone numbers, government-issued IDs, financial and credit-related information, account credentials, employment information, biometric data, precise geolocation data, and other sensitive PII.

33. As of April 16, 2026, Defendant has not provided formal notice of the Data Breach.

C. Impact of the Data Breach

34. The actual extent and scope, and the impact, of the Data Breach on Defendant's customers (or other affiliated persons) remains uncertain. Unfortunately for Plaintiff and Class Members, the damage is already done because their sensitive Personal Information has been disclosed to unauthorized persons during the Data Breach.

35. Defendant knew or should have known that its affected IT systems and/or servers are unsecure and do not meet industry standards for protecting highly sensitive customer Personal

[18] *See Cyberattacks' Unpredictable Targeting Remain Iran Risk*, GovInfoSecurity (Mar. 6, 2026), https://www.govinfosecurity.com/cyberattacks-unpredictable-targeting-remain-iran-risk-a-30930.

[19] *See 313 Team Threat Advisory: The 313 Team Wiper Attack*, HawkEye Threat Intelligence (Mar. 2026), https://hawk-eye.io/wp-content/advisories/313team-threat-advisory.html.

[20] *See Chime Goes Down for Thousands of Users*, *supra* n. 14.

Information. On information and belief, Defendant failed to implement reasonable measures to its data security systems, privacy policies, and its IT systems and servers, exposing its customers' Personal Information to the risk of theft, identity theft, and fraud.

36. The harm caused to Plaintiff and Class Members by the Data Breach has already been suffered.

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

38. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[21] TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[22]

39. Defendant had a duty to keep Plaintiff's and Class Members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal Information to Defendant with the understanding that Defendant would comply with its privacy policies and its obligations to keep such information confidential and secure from unauthorized disclosures.

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

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

40. Defendant's data security obligations were particularly important given the substantial increase in data breaches in recent years.

D. Theft of Personal Information Has Serious Consequences for Victims

41. Data breaches are by no means new, and they should not be unexpected. Business Insider has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[23] It is well known amongst companies that store sensitive personally identifying information that sensitive Personal Information—like SSNs, financial information, tax information, etc.—is valuable and frequently targeted by criminals.

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

43. Theft of Personal Information is serious. The Federal Trade Commission has warned consumers that identity thieves use Personal Information to exhaust financial accounts, receive services, start new utility accounts, and incur charges and credit in a person's name.[24]

44. Indeed, with access to an individual's Personal Information, criminals can do more than simply empty a victim's bank account. They can also commit all manner of fraud, including: obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; obtain lending or lines of credit; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[25]

---

[23] Dennis Green et al., *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[24] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 24, 2025).

[25] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 24, 2025).

45. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[26]

46. Personal Information is a valuable property right.[27] The value of sensitive personal information as a commodity is measurable.[28] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[29]

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

---

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

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

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

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

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

49. Consumers place a high value on the privacy of sensitive data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[30]

50. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[31]

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

52. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[32]

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

---

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

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

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

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

54. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other similar data breaches, Defendant failed to take reasonable steps to adequately protect the sensitive Personal Information in its possession, leaving its customers and other affiliated individuals exposed to risk of fraud and identity theft.

55. Defendant is, and at all relevant times has been, aware that the Personal Information it handles and stores in connection with providing its products and services is highly sensitive. As a company that collects and utilizes highly sensitive and identifying information in connection with providing financial products and services, Defendant is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

56. Defendant was aware, or should have been aware, of regulatory and industry guidance regarding data security, and was alerted to the risk associated with failing to ensure that Personal Information in its possession was adequately secured.

57. Despite the well-known risks of hackers and cybersecurity intrusions, Defendant failed to employ adequate data security measures in a meaningful way in order to prevent breaches, including the Data Breach.

58. The security flaws inherent to Defendant's IT systems or servers run afoul of industry best practices and standards. Had Defendant adequately protected and secured its servers or systems, and the sensitive Personal Information stored therein, it could have prevented the Data Breach.

59. Despite the fact that Defendant was on notice of the very real possibility of data theft, it still failed to implement adequate security measures and permitted a massive intrusion to occur that resulted in disclosure of Plaintiff's and other Class Members' Personal Information to criminals.

60. Defendant permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

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

through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[33]

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

63. Victims of the Data Breach are subject to an imminent and ongoing risk of harm, including identity theft and fraud.

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

CLASS ALLEGATIONS

65. Plaintiff brings this action individually and as a class action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) on behalf of himself and the following Classes:

> **Nationwide Class**
> All persons residing in the United States whose Personal Information was compromised in the Data Breach.
>
> **California Subclass**
> All persons residing in California whose Personal Information was compromised in the Data Breach.

66. The Nationwide Class and California Subclass are referred to herein as the "Class".

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

67. Excluded from the Class are Defendant, including any entity in which any Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by any Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of any Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families. Plaintiff reserves the right to expand, limit, modify, or amend the proposed Class definition before the Court determines whether certification is appropriate.

68. The Class meets the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the following reasons.

69. Numerosity. Although the exact number of Class members is uncertain, and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable, believed to amount to tens of thousands of persons. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and the Court. Information concerning the exact size of the putative class is within the possession of Defendant. The parties will be able to identify each member of the Class through discovery, including through Defendant's document production and/or related discovery.

70. Commonality. There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII.

b. Whether Defendant breached its duty to protect Plaintiff's and Class Members' PII.

c. Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;

d. Whether Defendant's data security systems prior to the Data Breach met industry standards;

e. Whether the actions and/or inaction of Defendant caused Plaintiff's and Class Members' PII to be disclosed or compromised;

f. Whether Defendant was negligent;

g. Whether Plaintiff and other Class Members are entitled to injunctive relief; and

h. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

71. Typicality. All of Plaintiff's claims are typical of the claims of the proposed Class he seeks to represent in that: Plaintiff's claims arise from the same practice or course of conduct that forms the basis of the Class claims; Plaintiff's claims are based upon the same legal and remedial theories as the proposed Class and involve similar factual circumstances; there is no antagonism between the interests of Plaintiff and absent Class Members; the injuries that Plaintiff suffered are similar to the injuries that Class Members have suffered.

72. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel experienced in complex class action litigation, including data breach and consumer protection cases. Plaintiff has no interests that are contrary to or in conflict with those of the Class.

73. Predominance. The proposed class action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Class predominate over any questions which may affect only individual Class members.

74. Superiority. The proposed class action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member. Absent a class action, the majority of Class Members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

75. Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant. Varying adjudications could establish incompatible standards with respect to: whether Defendant's ongoing conduct violates the claims alleged herein; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other Class Members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

76. Injunctive Relief. This action also satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making injunctive and declaratory relief appropriate with respect to the Class as a whole. Class Members continue to face ongoing harm from the exposure of their PII and require injunctive relief to address Defendant's inadequate security practices, breach response, and failure to prevent ongoing dissemination of highly sensitive PII.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

77. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

78. Defendant required Plaintiff and the Class Members to submit highly sensitive, non-public PII to Defendant in order to obtain products and services from Chime.

79. Defendant owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff's and Class Members' PII within its control from being compromised by or being accessed by unauthorized third parties. This duty arose from multiple sources, beginning with Defendant's voluntary assumption of this duty by promising to protect PII in its public facing privacy notice and disclosures.

80. The duty was further established by the special relationship created when Defendant required Plaintiff and Class Members to provide highly sensitive PII as a condition of obtaining Defendant's products and services. The foreseeable harm that would result from a breach of such sensitive information.

81. Defendant alone was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and other Class members from the Data Breach.

82. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act ("FTCA"), 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.

83. Defendant's duty to use reasonable care in protecting the PII arose not only as a result of the common law and the statutes and regulations described above, but also because it is bound by, and has committed to comply with, industry standards for the protection of confidential information.

84. Defendant breached its common law, statutory, and other duties—and thus, was negligent—by failing to use reasonable measures to protect its customers' PII, and by failing to provide timely notice of the Data Breach. 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 Plaintiff's and the Class Members' PII;

b. failing to adequately monitor the security of its networks and systems; and

c. allowing unauthorized access to Plaintiff's and the Class Members' PII.

85. Defendant owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

86. It was foreseeable that Defendant's failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

87. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

88. Defendant breached its duties of care through a cascade of failures. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the PII of Plaintiff and

members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the PII. Defendant unlawfully breached its duty to use reasonable care to protect and secure the PII of Plaintiff and the Class by representing to consumers that it maintained adequate data security, and then failing to implement basic security measures to protect Plaintiff's and Class Members' PII.

89. Defendant's breach was a substantial factor in causing Plaintiff's and Class Members' injuries. But for Defendant's failure to implement basic security measures, the breach would not have occurred.

90. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, among other things; (1) the exposure of their PII, including identification information such as home addresses, to online threat actors; (2) the loss of the ability to control how their PII is used; (3) compromise, publication and/or theft of Plaintiff's and Class Members' PII; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the Data Breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from PII misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) continued risks to their PII, which remains in Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its possession; and (8) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the PII compromised as a result of the Data Breach for the remainder of the Plaintiff's and Class Members' lives.

91. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

92. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

93. Defendant's duties arise from, *inter alia*, Section 5 of the FTCA, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Chime, of failing to employ reasonable measures to protect and secure PII.

94. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class Members' PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and other Class Members.

95. Defendant's violation of Section 5 of the FTCA constitutes negligence *per se*.

96. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

97. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and other Class Members as a result of the Data Breach.

98. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

99. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of,

inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

THIRD CAUSE OF ACTION
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiff and the Nationwide Class)

100. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

101. The Restatement (Second) of Torts 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).

102. Plaintiff and the Class Members had a reasonable expectation of privacy in the Personal Information that Defendant disclosed without authorization.

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

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

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

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

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

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

105. Defendant knew that its IT systems and servers were vulnerable to data breaches prior to the Data Breach.

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

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

108. In failing to protect Plaintiff's and Class members' Personal Information, and in disclosing Plaintiff's and Class members' Personal Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private.

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

FOURTH CAUSE OF ACTION

Invasion of Privacy, Cal. Const. ART. 1 § 1
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the California Subclass)

110. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

111. California established the right to privacy in Article I, Section 1 of the California Constitution.

112. Plaintiff and Class Members had a legitimate expectation of privacy to their Personal Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

113. Defendant owed a duty to their customers, including Plaintiff and Class Members, to keep their Personal Information contained as a part thereof, confidential.

114. Defendant failed to protect and released Plaintiff's and Class Members' Personal Information to unknown and unauthorized third parties.

115. Defendant allowed unauthorized and unknown third parties access to and examination of Plaintiff's and Class Members' Personal Information, by way of Defendant's failure to protect that Personal Information.

116. The unauthorized release to, custody of, and examination by unauthorized third parties of Plaintiff's and Class Members' Personal Information is highly offensive to a reasonable person.

117. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Personal Information to Defendant in connection with seeking financial services from Defendant, but privately with an intention that the Personal Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

118. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

119. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

120. Because Defendant acted with a knowing state of mind, it had notice that its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

121. As a proximate result of Defendant's acts and omissions, the Personal Information of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

122. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Personal Information maintained by Defendant can be viewed, distributed, and used by unauthorized

persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

FIFTH CAUSE OF ACTION

Breach Of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

123. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

124. Plaintiff and members of the Class were required to provide, and did provide, their PII to Defendant as a condition of obtaining products and services from Chime.

125. Plaintiff and members of the Class had no alternative and did not have any bargaining power with regard to providing their PII. Defendant required disclosure of their PII as a condition to access and use of Defendant's products and services, which the Plaintiff and members of the Class did.

126. When Plaintiff and Class Members provided their PII to Defendant in exchange for access and use of Defendant's products and services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such PII and to timely and accurately notify them if their data had been breached and compromised.

127. Defendant solicited prospective customers to provide their PII as part of its regular business practices. These individuals accepted Defendant's offers and provided their PII to Defendant. In entering into such implied contracts, Plaintiff and the Class reasonably assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

128. Plaintiff and the Class would not have provided and entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

129. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

130. Defendant breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Data Breach.

131. As a direct and proximate result of Defendant's breaches of its implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

132. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION

Violations of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200 et seq.
(On Behalf of Plaintiff and the Nationwide Class)

133. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

134. Defendant is a "person" as that term is defined by, *inter alia*, Cal. Bus. & Prof. Code § 17201.

135. Defendant violated the California Unfair Competition Law ("UCL"), §§ 17200, *et seq*., by engaging in unlawful, unfair, and deceptive business acts and practices.

136. Defendant's unlawful, unfair, and deceptive acts and practices include Defendant's failure to implement and maintain reasonable data security policies, practices, and measures to protect the PII of Plaintiff and Class Members from unauthorized access, disclosure, release, and theft, which was a direct and proximate cause of the Data Breach.

137. Defendant failed to:

a. Secure access to its computer systems and database;

b. Comply with relevant industry standards for data and network security practices;

c. Adequately secure or segment its company network(s);

d. Implement adequate system and event monitoring over its computer systems;

e. Timely update and patch relevant programs related to its computer systems; and

f. Implement the systems, policies, and procedures necessary to prevent a foreseeable security intrusion such as the Data Breach.

138. Defendant failed to identify and take adequate precautions against foreseeable security risks or to adequately improve its data security.

139. Defendant's lackluster security provides little, if any utility, and is particularly unfair within the meaning of the UCL when weighed against the resultant harm to Plaintiff and Class Members.

140. Defendant's lackluster security is also contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with it use appropriate security measures, as reflected in laws, including, *inter alia*, the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5, 1798.82, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*.

141. Defendant's failure to implement and maintain reasonable data security policies, procedures, and measures, and failures to prevent the dissemination of stolen PII lead to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition as contemplated under the UCL. Because Plaintiff and the Class Members did not and could not know of Defendant's inadequate security and compromise of their PII, they could not have reasonably avoided the harms caused by Defendant.

142. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, yet failed to do so. Defendant further omitted, suppressed, and/or concealed the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII.

143. Defendant misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including all such duties as imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*., yet failed to do so. Defendant further omitted, suppressed, and/or concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including the duties imposed by the aforementioned statutes.

144. Defendant engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

145. Defendant's misrepresentations and omissions to Plaintiff and the Class Members were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and ability to protect the privacy of their PII.

146. Defendant intended to mislead Plaintiff and members of the Class and induce them to rely on its misrepresentations and omissions.

147. If Defendant had disclosed to Plaintiff and members of the Class that its computer and data systems were not secure and, thus, vulnerable to cyberattack, Defendant would have been unable to continue in business with such inadequate security policies, practices, and measures, and it would have been forced to adopt reasonable cybersecurity measures, in compliance with the law. However, Defendant instead received, maintained, and compiled Plaintiff's and the Class Members' PII as a condition of using its services without advising Plaintiff and Class Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the veracity of which they could not have discovered prior to the Data Breach.

148. Defendant acted intentionally, knowingly, and maliciously to violate the UCL in reckless disregard of Plaintiff's and Class Members' rights.

149. As a direct and proximate result of Defendant's violations of the UCL, Plaintiff and the Class sustained actual losses and damages as described herein.

150. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

151. Plaintiff brings this Cause of Action on behalf of all Class Members pursuant to UCL § 17203, which authorized extraterritorial application of the UCL.

SEVENTH CAUSE OF ACTION

Violation Of The California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the California Subclass)

152. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

153. The California Legislature enacted the California Customer Records Act ("CRA"), Cal. Civ. Code §§ 1798.80, *et seq*., "to ensure that Personal Information about California residents is protected." Cal. Civ. Code § 1798.81.5(a)(1).

154. The CRA requires that "[a] business that owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices

appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

155. Defendant maintains computerized data that includes PII, as defined by Cal. Civ. Code § 1798.80. This includes PII about Plaintiff and Class Members that was disclosed in the Data Breach. Cal. Civ. Code § 1798.81.5(d)(1)(A); Cal. Civ. Code § 1798.82.

156. Pursuant to the CRA, Defendant was required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). 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." Cal. Civ. Code § 1798.82.

157. Defendant reasonably believed that Plaintiff's and the California Subclass Members' PII was acquired by unauthorized persons during the Data Breach. As such, Defendant had an obligation under the CRA to disclose the Data Breach, immediately following its discovery, to Plaintiff and California Subclass Members as the owners or licensees of the PII. Cal. Civ. Code § 1798.82.

158. By willfully, intentionally, and/or recklessly failing to disclose the Data Breach immediately following its discovery, Defendant violated Cal. Civ. Code § 1798.82.

159. As a direct and proximate result of Defendant's violations of the CRA, Plaintiff and the California Subclass sustained actual losses and damages as described herein.

160. Plaintiff and the California Subclass seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

EIGHTH CAUSE OF ACTION

Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.150 *et seq.* ("CCPA")
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the California Subclass)

161. Plaintiff incorporates the foregoing allegations as if fully set forth herein

162. This claim is pleaded on behalf of Plaintiff and the California Sub-Class.

163. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to

implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

164. Defendant is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

165. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

166. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g).

167. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because it is a corporation that does business in the state of California and has annual revenues of in excess of $25,000,000.

168. Plaintiff's name in combination and other sensitive PII, compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA. *See* Civ. Code § 1798.150(a)(1).

169. Through the Data Breach, Plaintiff's PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

170. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

171. In accordance with Cal. Civ. Code § 1798.150(b)(1), prior to the filing of this Complaint, Plaintiff's counsel served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

172. If Defendant fails to respond to Plaintiff's notice letter or agree to rectify the violations detailed above and give notice to all affected consumers within 30 days of the date of written notice, Plaintiff also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

NINTH CAUSE OF ACTION

Declaratory and Injunctive Relief
(On Behalf of Plaintiff and the Nationwide Class)

173. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

174. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court may enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Moreover, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

175. An actual controversy exists between Plaintiff and Class members on one hand, and Defendant on the other, regarding Defendant's data security practices and duties going forward.

176. The harm to Plaintiff and Class members is ongoing and irreparable. Their PII remains exposed on the internet and to cybercriminals. They face continuing risks of identity theft, fraud, stalking, and harassment. Without injunctive relief, Defendant is likely to continue its inadequate practices, putting current and future consumers at risk.

177. Plaintiff and Class members have no adequate remedy at law. Money damages cannot undo the exposure of their PII or eliminate the ongoing risks they face. Only prospective relief can prevent further harm and ensure Defendant implements adequate measures.

178. Plaintiff seeks a declaration that:

a. Defendant's data security practices violated and continue to violate its legal obligations;

b. Defendant has obligations to prevent the dissemination of stolen personal information on its platforms;

c. Defendant must implement comprehensive measures to protect consumers from data breaches and their consequences;

d. Defendant must delete all unnecessary Personal Information in its possession;

e. Defendant must provide transparent disclosures about its practices;

f. Defendant must submit to regular audits by qualified third parties.

179. Plaintiff further seeks injunctive relief requiring Defendant to implement comprehensive remedial measures. Plaintiff seeks an order requiring immediate implementation of comprehensive

information security measures, including encryption of all PII at rest and in transit, access controls limiting who can view sensitive data, regular security audits and penetration testing, employee training on data security, incident response procedures, and data minimization and retention policies. Defendant must also delete all personal information that is no longer necessary for legitimate business purposes, provide clear and conspicuous notice to consumers about what data is collected, how it is used, how long it is retained, and how it is protected, implement a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information, and engage third-party security auditors to assess compliance and publish the results.

180. Plaintiff and Class Members continue to suffer injury as a result of Defendant's negligent exposure of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

181. Additionally, Plaintiff's and Class Members' PII, when contained in electronic form, is highly attractive to criminals who can nefariously use their PII for fraud, identity theft, and other crimes without their knowledge and consent.

182. As alleged herein, the failures of the Defendant to implement adequate cyber-security measures and protocols has led to the compromise of Plaintiff's and Class Members' PII. Plaintiff and members of the Class were required to provide as a condition of obtaining services from Defendant, resulting in irreparable harm.

183. Defendant remains in possession of Plaintiff's and Class Members' PII. It is imperative that the Court intervene to assure that the Defendant takes all reasonable steps to protect that PII lest there be another data breach.

184. The balance of equities tips decidedly in Plaintiff's favor. The burden on Defendant of implementing proper security measures is minimal compared to the enormous ongoing harm to Class members from continued exposure of their personal information.

185. Injunctive relief would serve the public interest by protecting consumers' personal information, preventing the weaponization of data breaches, and enforcing minimum standards for companies that collect sensitive data and platforms that can amplify harm.

186. The hardship to Plaintiff and Class Members if such an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Absent an injunction, Plaintiff will likely be subjected to substantial identity theft and other damages, whereas the cost to Defendant of complying with an injunction by employing reasonable data security policies, practices, and measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment on behalf of himself and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing Plaintiff as Class representative and the undersigned counsel as Class Counsel to represent the putative Class;

b. Awarding Plaintiff and the Class appropriate relief, including actual damages, compensatory damages, and punitive damages, as allowed by law;

c. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

d. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

e. Awarding Plaintiff and the Class prejudgment and post-judgment interest;

f. Awarding Plaintiff and the Class their attorneys' fees and costs, as allowable by law; and

g. Awarding such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the Class, demands a trial by jury as to all issues triable of right.

DATED: April 17, 2026

Respectfully submitted,

/s/ Tina Wolfson

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Jeff S. Westerman (SBN 94559)
jwesterman@ahdootwolfson.com
Lisa M. Cintron (SBN 356009)
lcintron@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500

Burbank, California 91505
Tel: 310-474-9111
Fax: 310-474-8585

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

Counsel for Plaintiff and the Proposed Class