

1 Carly M. Roman (No. 349895)
2 croman@straussborrelli.com
3 **STRAUSS BORRELLI PLLC**
4 980 N. Michigan Ave., Suite 1610
5 Chicago, IL 60611
6 2261 Market St., Ste. 22946
7 San Francisco, CA 94114
8 Telephone: (872) 263-1100
9 Facsimile: (872) 263-1109
10 *Attorney for Plaintiffs and Proposed Class*

11 **UNITED STATES DISTRICT COURT**
12 **NORTHERN DISTRICT OF CALIFORNIA**

13 **CINDY CASTANEDA and LAUREN**
14 **GOODLOE**, on behalf of themselves and all
15 others similarly situated,

16 Plaintiffs,

17 v.

18 **CHIME FINANCIAL, INC.**,

19 Defendant.

Case No. 3:26-cv-2924

CLASS ACTION COMPLAINT

- 1. NEGLIGENCE;
- 2. NEGLIGENCE *PER SE*;
- 3. BREACH OF IMPLIED CONTRACT;
- 4. BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
- 5. UNJUST ENRICHMENT
- 6. CALIFORNIA’S UNFAIR COMPETITION LAW;
- 7. CALIFORNIA CONSUMER PRIVACY ACT; AND
- 8. DECLARATORY JUDGMENT.

DEMAND FOR JURY TRIAL

22
23 Cindy Castaneda and Lauren Goodloe (“Plaintiffs”), through their attorneys, individually
24 and on behalf of all others similarly situated, brings this Class Action Complaint against
25 Defendant Chime Financial, Inc. (“Chime” or “Defendant”), and its present, former, or future
26 direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities.

1 Plaintiffs allege the following on information and belief—except as to their own actions,
2 counsel’s investigations, and facts of public record.

3 **NATURE OF ACTION**

4 1. This class action arises from Defendant’s failure to protect highly sensitive data.

5 2. Defendant is a financial technology company offering a suite of app-based banking
6 and financial services through partnerships with FDIC-insured banks.¹

7 3. As such, Defendant store a litany of highly sensitive personal identifiable
8 information (“PII”) about its customers. But Defendant lost control over that data when
9 cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the “Data
10 Breach”).

11 4. An unauthorized actor gained access to Defendant’s systems on or about April 1,
12 2026. Thus, cybercriminals had unfettered access to Defendant’s network and the files stored
13 therein and caused a widespread outage in Defendant’s services.

14 5. Reports stated that, “[t]housands of users across the United States reported
15 problems Wednesday with logging in, accessing balances, sending money and using the
16 mobile app.”² Some customers reported being unable to access their funds during the disruption.³

17 6. In other words, Defendant had no effective means to prevent, detect, stop, or
18 mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its
19 current and former customers’ PII and causing a platform-wide disruption in services.

20 7. On information and belief, cybercriminals were able to breach Defendant’s
21 systems because Defendant failed to adequately train its employees on cybersecurity and failed
22 to maintain reasonable security safeguards or protocols to protect the Class’s PII. In short,
23

24
25 ¹ About, Chime, <https://www.chime.com/about-us/> (last visited April 3, 2026).

26 ² Is Chime Down? What Users Should Know About Funds and Personal Data, Newsweek,
<https://www.newsweek.com/chime-down-outage-service-status-not-working-11770861> (last
27 visited April 3, 2026).

³ *Id.*

1 Defendant’s failures placed the Class’s PII in a vulnerable position—rendering them easy targets
2 for cybercriminals.

3 8. Plaintiffs are current customers of Defendant and Data Breach victims. They bring
4 this class action on behalf of themselves, and all others harmed by Defendant’s misconduct.

5 9. The exposure of one’s PII to cybercriminals is a bell that cannot be unrung. Before
6 this data breach, its current and former customers’ private information was exactly that—private.
7 Not anymore. Now, their private information is forever exposed and unsecure.

8 **PARTIES**

9 10. Plaintiff, Cindy Castaneda, is a natural person and citizen of Madera, California
10 where she intends to remain.

11 11. Plaintiff, Lauren Goodloe, is a natural person and citizen of Chicago, Illinois
12 where he intends to remain.

13 12. Defendant, Chime Financial, Inc., is a stock corporation formed under the laws of
14 Delaware and with its principal place of business at 101 California Street, Suite 500, San
15 Francisco, CA 94111.

16 **JURISDICTION AND VENUE**

17 13. This Court has subject matter jurisdiction over this action under the Class Action
18 Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive
19 of interest and costs. Defendant and at least one class member are citizens of different states. And
20 there are over 100 putative Class Members.

21 14. This Court has personal jurisdiction over Defendant because Chime has its
22 principal place of business and/or corporate headquarters in California. Furthermore, Defendant
23 regularly conducts business in California and has sufficient minimum contacts in California.

24 15. Venue is proper in this Court because Defendant’s principal office is in this
25 District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs’
26 claims occurred in this District.

1 **BACKGROUND**

2 ***Defendant Collected and Stored the PII of Plaintiffs and the Class***

3 16. Defendant is a financial technology company offering a suite of app-based banking
4 and financial services through partnerships with FDIC-insured banks.⁴

5 17. As part of its business, Defendant receives and maintains the PII of thousands of
6 its customers.

7 18. In collecting and maintaining the PII, Defendant agreed it would safeguard the
8 data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and
9 Class Members themselves took reasonable steps to secure their PII.

10 19. Under state and federal law, businesses like Defendant have duties to protect their
11 current and former customers' PII and to notify them about breaches.

12 20. Defendant recognizes these duties, promising in its "Privacy Notice" that "[w]e
13 maintain administrative, technical and physical safeguards designed to protect the personal
14 information you provide against accidental, unlawful or unauthorized access, destruction, loss,
15 alteration, disclosure or use."⁵

16 21. In collecting and maintaining customers' PII, Defendant agreed it would safeguard
17 the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and
18 Class Members themselves took reasonable steps to secure their PII.

19 22. Despite recognizing its duty to do so, on information and belief, Defendant has not
20 implemented reasonably cybersecurity safeguards or policies to protect its former and current
21 employees' and students' PII or supervised its IT or data security agents and employees to prevent,
22 detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in
23 its systems for cybercriminals to exploit and gain access to customers' PII.

24 ***Defendant's Data Breach***

25 _____
26 ⁴ About, Chime, <https://www.chime.com/about-us/> (last visited April 3, 2026).

27 ⁵ Chime U.S. Privacy Notice, Chime, <https://www.chime.com/policies/chime/privacy-policy/#how-we-protect-personal-information> (last visited April 3, 2026).

1 23. On or around April 1, 2026, Defendant experienced a widespread outage on its
2 network due to unauthorized access to its systems by cybercriminals.

3 24. Reports stated that, “[t]housands of users across the United States reported
4 problems Wednesday with logging in, accessing balances, sending money and using the
5 mobile app.”⁶ Some customers reported being unable to access their funds during the disruption.⁷

6 25. Defendant has yet to formally notify Class Members of the Breach even though
7 Plaintiffs and thousands of Class Members had their most sensitive personal information
8 accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss
9 of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate
10 the effects of the attack.

11 26. Defendant failed its duties when its inadequate security practices caused the Data
12 Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent the Data
13 Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread
14 injury and monetary damages.

15 27. Because of Defendant’s Data Breach, the sensitive PII of Plaintiffs and Class
16 Members was placed into the hands of cybercriminals—inflicting numerous injuries and
17 significant damages upon Plaintiffs and Class Members.

18 28. Upon information and belief, cybercriminal group Team 313 was responsible for
19 the Data Breach.⁸

20 29. Team 313 is known for employing data theft and extortion, and operating data leak
21 sites where it publishes stolen data in order to pressure organizations who were subject to a data
22 breach.⁹ It is reported that Team 313’s “operational model fuses technical compromise with rapid
23

24 ⁶ Is Chime Down? What Users Should Know About Funds and Personal Data, Newsweek,
25 <https://www.newsweek.com/chime-down-outage-service-status-not-working-11770861> (last
visited April 3, 2026).

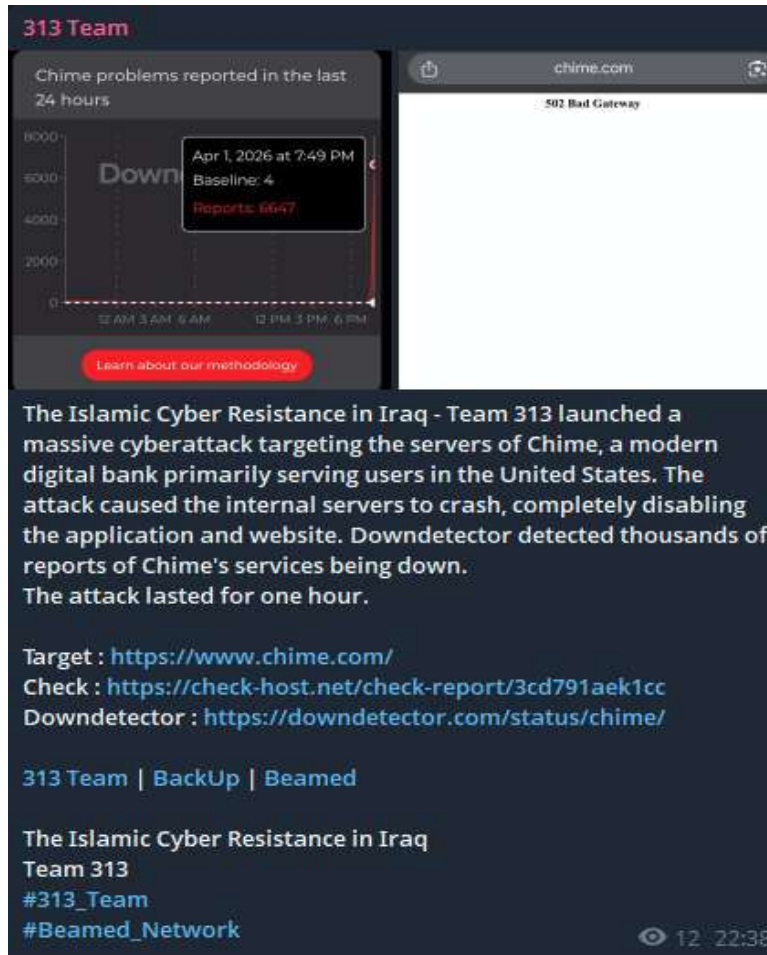
26 ⁷ *Id.*

27 ⁸ @FalconFeeds.io, TWITTER (X) (April 1, 2026, 1:43 PM).

28 ⁹ 313 Team Threat Advisory: The 313 Team Wiper Attack, Hawkeye,

1 public messaging, timed data leaks, and narrative amplification designed to maximize
 2 reputational damage beyond direct system impact.”¹⁰

3 30. Team 313 posted on its leak site that it “launched a massive cyberattack targeting
 4 the servers of Chime...The attack caused the internal servers to crash, completely disabling the
 5 application and website. Downtdetector detected thousands of reports of Chime’s services being
 6 down.”¹¹ The post also contained an icon demonstrating that it had been viewed at least 12 times.¹²



23 _____
 24 <https://hawk-eye.io/wp-content/advisories/313team-threat-advisory.html> (last visited April 3,
 2026).

25 ¹⁰ 313 Team Threat Advisory: The 313 Team Wiper Attack, Hawkeye,
 26 <https://hawk-eye.io/wp-content/advisories/313team-threat-advisory.html> (last visited April 3,
 2026).

27 ¹¹ @FalconFeeds.io, TWITTER (X) (April 1, 2026, 1:43 PM).

28 ¹² *Id.*

1 31. This indicates that Team 313 hacked Defendant’s network, stole sensitive PII
2 contained therein, and published the stolen PII on the dark web.

3 32. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use
4 the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have
5 gained unauthorized access to through credential stuffing attacks, phishing attacks, [or]
6 hacking.”¹³

7 33. Thus, on information and belief, Plaintiffs’ and the Class’s stolen PII has already
8 been published—or will be published imminently—by cybercriminals on the Dark Web.

9 ***Plaintiff Cindy Castaneda’s Experiences and Injuries***

10 34. Plaintiff Cindy Castaneda is a current customer of Defendant and is a Data Breach
11 victim.

12 35. As a condition of receiving services from Defendant, Plaintiff Castaneda provided
13 Defendant with her PII. Defendant used that PII to facilitate its provision of services.

14 36. Thus, Defendant obtained and maintained Plaintiff Castaneda’s PII.

15 37. As a result, Plaintiff Castaneda was injured by Defendant’s Data Breach.

16 38. Plaintiff Castaneda provided her PII to Defendant and trusted the company would
17 use reasonable measures to protect it according to Defendant’s internal policies, as well as state
18 and federal law. Defendant obtained and continues to maintain Plaintiff’s PII and has a continuing
19 legal duty and obligation to protect that PII from unauthorized access and disclosure.

20 39. Through its Data Breach, Defendant compromised Plaintiff Castaneda’s PII and
21 caused a disruption in her services. Indeed, on April 1, 2026, Plaintiff was unable to see her
22 updated balance of her checking and savings account in the Chime mobile app.

23 40. Thus, on information and belief, Plaintiff Castaneda’s PII has already been
24 published—or will be published imminently—by cybercriminals on the Dark Web.

25
26 ¹³ Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It*
27 *Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

1 41. Plaintiff Castaneda does not recall ever learning that her information was
2 compromised in a data breach incident—other than the breach at issue here.

3 42. Plaintiff Castaneda has spent—and will continue to spend—significant time and
4 effort researching the data breach, monitoring her accounts to protect herself from identity theft,
5 and contacting counsel.

6 43. Plaintiff Castaneda fears for her personal financial security and worries about what
7 information was exposed in the Data Breach.

8 44. Because of Defendant’s Data Breach, Plaintiff Castaneda has suffered—and will
9 continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go
10 far beyond allegations of mere worry or inconvenience. Rather, Plaintiff’s injuries are precisely
11 the type of injuries that the law contemplates and addresses.

12 45. Plaintiff Castaneda suffered actual injury from the exposure and theft of her PII—
13 which violates her rights to privacy.

14 46. Plaintiff Castaneda suffered actual injury in the form of damages to and diminution
15 in the value of her PII. After all, PII is a form of intangible property—property that Defendant
16 were required to adequately protect.

17 47. Plaintiff Castaneda suffered imminent and impending injury arising from the
18 substantially increased risk of fraud, misuse, and identity theft—all because Defendant’s Data
19 Breach placed Plaintiff’s PII right in the hands of criminals.

20 48. Because of the Data Breach, Plaintiff Castaneda anticipates spending considerable
21 amounts of time and money to try and mitigate her injuries.

22 49. Today, Plaintiff Castaneda has a continuing interest in ensuring that her PII—
23 which, upon information and belief, remains backed up in Defendant’s possession—is protected
24 and safeguarded from additional breaches.

25 ***Plaintiff Lauren Goodloe’s Experiences and Injuries***

1 50. Plaintiff Lauren Goodloe is a current customer of Defendant and is a Data Breach
2 victim.

3 51. As a condition of receiving services from Defendant, Plaintiff Goodloe provided
4 Defendant with his PII. Defendant used that PII to facilitate its provision of services.

5 52. Thus, Defendant obtained and maintained Plaintiff Goodloe's PII.

6 53. As a result, Plaintiff Goodloe was injured by Defendant's Data Breach.

7 54. Plaintiff Goodloe provided his PII to Defendant and trusted the company would
8 use reasonable measures to protect it according to Defendant's internal policies, as well as state
9 and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing
10 legal duty and obligation to protect that PII from unauthorized access and disclosure.

11 55. Through its Data Breach, Defendant compromised Plaintiff Goodloe's PII and
12 caused a disruption in his services. Indeed, on April 1, 2026, when Plaintiff logged into his
13 account on the Chime app to pay his rent, he could see only a black screen with an outdated
14 balance for his savings account. Plaintiff was unable to see any up-to-date account balances, view
15 any updated transactions, transfer money in or out of his account, or pay his bills. As a result,
16 Plaintiff was unable to pay his rent on time because (1) he was unable to see an updated balance
17 and was concerned that paying his rent might over draw his account and (2) he was unable to
18 transfer money to his account. Plaintiff is concerned he may receive late fees because of his
19 delayed rent payment.

20 56. Thus, on information and belief, Plaintiff Goodloe's PII has already been
21 published—or will be published imminently—by cybercriminals on the Dark Web.

22 57. Plaintiff Goodloe does not recall ever learning that his information was
23 compromised in a data breach incident—other than the breach at issue here.

24 58. Plaintiff Goodloe has spent—and will continue to spend—significant time and
25 effort researching the data breach, monitoring his accounts to protect himself from identity theft,
26 and contacting counsel.

1 59. Plaintiff Goodloe fears for his personal financial security and worries about what
2 information was exposed in the Data Breach.

3 60. Because of Defendant’s Data Breach, Plaintiff Goodloe has suffered—and will
4 continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go
5 far beyond allegations of mere worry or inconvenience. Rather, Plaintiff’s injuries are precisely
6 the type of injuries that the law contemplates and addresses.

7 61. Plaintiff Goodloe suffered actual injury from the exposure and theft of his PII—
8 which violates his rights to privacy.

9 62. Plaintiff Goodloe suffered actual injury in the form of damages to and diminution
10 in the value of his PII. After all, PII is a form of intangible property—property that Defendant
11 were required to adequately protect.

12 63. Plaintiff Goodloe suffered imminent and impending injury arising from the
13 substantially increased risk of fraud, misuse, and identity theft—all because Defendant’s Data
14 Breach placed Plaintiff’s PII right in the hands of criminals.

15 64. Because of the Data Breach, Plaintiff Goodloe anticipates spending considerable
16 amounts of time and money to try and mitigate his injuries.

17 65. Today, Plaintiff Goodloe has a continuing interest in ensuring that his PII—which,
18 upon information and belief, remains backed up in Defendant’s possession—is protected and
19 safeguarded from additional breaches.

20 ***Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft***

21 66. Because of Defendant’s failure to prevent the Data Breach, Plaintiffs and Class
22 Members suffered—and will continue to suffer—damages. These damages include, *inter alia*,
23 monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an
24 increased risk of suffering:

- 25 a. loss of the opportunity to control how their PII is used;
26 b. diminution in value of their PII;

- 1 c. compromise and continuing publication of their PII;
- 2 d. out-of-pocket costs from trying to prevent, detect, and recovery from
- 3 identity theft and fraud;
- 4 e. lost opportunity costs and wages from spending time trying to mitigate the
- 5 fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting,
- 6 and recovering from identify theft and fraud;
- 7 f. delay in receipt of tax refund monies;
- 8 g. unauthorized use of their stolen PII; and
- 9 h. continued risk to their PII—which remains in Defendant’s possession—
- 10 and is thus as risk for futures breaches so long as Defendant fail to take
- 11 appropriate measures to protect the PII.

12 67. Stolen PII is one of the most valuable commodities on the criminal information
13 black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to
14 \$1,000.00 depending on the type of information obtained.

15 68. The value of Plaintiffs’ and Class’s PII on the black market is considerable. Stolen
16 PII trades on the black market for years. And criminals frequently post and sell stolen information
17 openly and directly on the “Dark Web”—further exposing the information.

18 69. It can take victims years to discover such identity theft and fraud. This gives
19 criminals plenty of time to sell the PII far and wide.

20 70. One way that criminals profit from stolen PII is by creating comprehensive
21 dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and
22 comprehensive. Criminals create them by cross-referencing and combining two sources of data—
23 first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone
24 numbers, emails, addresses, etc.).

25 71. The development of “Fullz” packages means that the PII exposed in the Data
26 Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

1 72. In other words, even if certain information such as emails, phone numbers, or
2 credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data
3 Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous
4 operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly
5 what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact,
6 including this Court or a jury, to find that Plaintiffs' and other Class Members' stolen PII is being
7 misused, and that such misuse is fairly traceable to the Data Breach.

8 73. Defendant disclosed the PII of Plaintiffs and Class Members for criminals to use
9 in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the
10 PII of Plaintiffs and Class Members to people engaged in disruptive and unlawful business
11 practices and tactics, including online account hacking, unauthorized use of financial accounts,
12 and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the
13 stolen PII.

14 74. Defendant's failure to promptly and properly notify Plaintiffs and Class Members
15 of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the
16 earliest ability to take appropriate measures to protect their PII and take other necessary steps to
17 mitigate the harm caused by the Data Breach.

18 ***Defendant Knew—Or Should Have Known—of the Risk of a Data Breach***

19 75. Defendant's data security obligations were particularly important given the
20 substantial increase in cyberattacks and/or data breaches in recent years.

21 76. In 2021, a record 1,862 data breaches occurred, exposing approximately
22 293,927,708 sensitive records—a 68% increase from 2020.¹⁴

23 77. Indeed, cyberattacks have become so notorious that the Federal Bureau of
24 Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are
25

26 ¹⁴ See 2021 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER (Jan. 2022)
27 <https://notified.idtheftcenter.org/s/>.

1 aware of, and prepared for, a potential attack.¹⁵

2 78. Therefore, the increase in such attacks, and attendant risk of future attacks, was
3 widely known to the public and to anyone in Defendant’s industry, including Defendant.

4 ***Consumers Prioritize Data Security***

5 79. In 2024, the technology and communications conglomerate Cisco published the
6 results of its multi-year “Consumer Privacy Survey.”¹⁶ Therein, Cisco reported the following:

- 7 a. “For the past six years, Cisco has been tracking consumer trends across the
8 privacy landscape. During this period, privacy has evolved from relative
9 obscurity to a customer requirement with more than 75% of consumer
10 respondents saying they won’t purchase from an organization they don’t
11 trust with their data.”¹⁷
- 12 b. “Privacy has become a critical element and enabler of customer trust, with
13 94% of organizations saying their customers would not buy from them if
14 they did not protect data properly.”¹⁸
- 15 c. 89% of consumers stated that “I care about data privacy.”¹⁹
- 16 d. 83% of consumers declared that “I am willing to spend time and money to
17 protect data” and that “I expect to pay more” for privacy.²⁰
- 18 e. 51% of consumers revealed that “I have switched companies or providers
19 over their data policies or data-sharing practices.”²¹
- 20

21 ¹⁵ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18,
22 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

23 ¹⁶ *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO,
24 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited June 24, 2025).

25 ¹⁷ *Id.* at 3.

26 ¹⁸ *Id.*

27 ¹⁹ *Id.* at 9.

28 ²⁰ *Id.*

²¹ *Id.*

1 f. 75% of consumers stated that “I will not purchase from organizations I don’t
2 trust with my data.”²²

3 ***Defendant Failed to Follow FTC Guidelines***

4 80. According to the Federal Trade Commission (“FTC”), the need for data security
5 should be factored into all business decision-making. Thus, the FTC issued numerous guidelines
6 identifying best data security practices that businesses—like Defendant—should use to protect
7 against unlawful data exposure.

8 81. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
9 *Guide for Business*. There, the FTC set guidelines for what data security principles and practices
10 businesses must use.²³ The FTC declared that, *inter alia*, businesses must:

- 11 a. protect the personal customer information that they keep;
- 12 b. properly dispose of personal information that is no longer needed;
- 13 c. encrypt information stored on computer networks;
- 14 d. understand its network’s vulnerabilities; and
- 15 e. implement policies to correct security problems.

16 82. The guidelines also recommend that businesses watch for the transmission of large
17 amounts of data out of the system—and then have a response plan ready for such a breach.

18 83. Furthermore, the FTC explains that companies must:

- 19 a. not maintain information longer than is needed to authorize a transaction;
- 20 b. limit access to sensitive data;
- 21 c. require complex passwords to be used on networks;
- 22 d. use industry-tested methods for security;
- 23 e. monitor for suspicious activity on the network; and
- 24 f. verify that third-party service providers use reasonable security measures.

25 ²² *Id.* at 11.

26 ²³ *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION (Oct.
27 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

1 84. The FTC brings enforcement actions against businesses for failing to protect
2 customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and
3 appropriate measures to protect against unauthorized access to confidential consumer data—as
4 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),
5 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must
6 take to meet its data security obligations.

7 85. In short, Defendant’s failure to use reasonable and appropriate measures to protect
8 against unauthorized access to its current and former customers’ data constitutes an unfair act or
9 practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

10 ***Defendant Failed to Follow Industry Standards***

11 86. Several best practices have been identified that—at a *minimum*—should be
12 implemented by businesses like Defendant. These industry standards include: educating all
13 employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-
14 malware software; encryption (making data unreadable without a key); multi-factor
15 authentication; backup data; and limiting which employees can access sensitive data.

16 87. Other industry standard best practices include: installing appropriate malware
17 detection software; monitoring and limiting the network ports; protecting web browsers and email
18 management systems; setting up network systems such as firewalls, switches, and routers;
19 monitoring and protection of physical security systems; protection against any possible
20 communication system; and training staff regarding critical points.

21 88. Upon information and belief, Defendant failed to implement industry-standard
22 cybersecurity measures, including failing to meet the minimum standards of both the NIST
23 Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02,
24 PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01,
25 PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-

1 04) and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are all
2 established standards in reasonable cybersecurity readiness.

3 89. These frameworks are applicable and accepted industry standards. And by failing
4 to comply with these accepted standards, Defendant opened the door to the criminals—thereby
5 causing the Data Breach.

6 **CLASS ACTION ALLEGATIONS**

7 90. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),
8 individually and on behalf of all members of the following class:

9 All individuals residing in the United States whose PII was
10 compromised in the Data Breach experienced by Chime in April
11 2026.

12 91. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries,
13 any entity in which Defendant have a controlling interest, any Defendant officer or director, any
14 successor or assign, and any Judge who adjudicates this case, including its staff and immediate
15 family.

16 92. Plaintiffs reserve the right to amend the class definition.

17 93. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because
18 Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as
19 would be used to prove those elements in individual actions asserting the same claims.

20 94. Ascertainability. All members of the proposed Class are readily ascertainable from
21 information in Defendant’s custody and control.

22 95. Numerosity. The Class Members are so numerous that joinder of all Class
23 Members is impracticable. Upon information and belief, the proposed Class includes at least
24 thousands of members.

25 96. Typicality. Plaintiffs’ claims are typical of Class Members’ claims as each arises
26 from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable
27 manner of notifying individuals about the Data Breach.

1 97. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class’s
2 common interests. Their interests do not conflict with Class Members’ interests. And Plaintiffs
3 have retained counsel—including lead counsel—that is experienced in complex class action
4 litigation and data privacy to prosecute this action on the Class’s behalf.

5 98. Commonality and Predominance. Plaintiffs’ and the Class’s claims raise
6 predominantly common fact and legal questions—which predominate over any questions
7 affecting individual Class Members—for which a class wide proceeding can answer for all Class
8 Members. In fact, a class wide proceeding is necessary to answer the following questions:

- 9 a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs’
10 and the Class’s PII;
- 11 b. if Defendant failed to implement and maintain reasonable security
12 procedures and practices appropriate to the nature and scope of the
13 information compromised in the Data Breach;
- 14 c. if Defendant were negligent in maintaining, protecting, and securing PII;
- 15 d. if Defendant breached contract promises to safeguard Plaintiffs and the
16 Class’s PII;
- 17 e. if Defendant took reasonable measures to determine the extent of the Data
18 Breach after discovering it;
- 19 f. if Defendant’s Breach Notice was reasonable;
- 20 g. if the Data Breach caused Plaintiffs and the Class injuries;
- 21 h. what the proper damages measure is; and
- 22 i. if Plaintiffs and the Class are entitled to damages, treble damages, and or
23 injunctive relief.

24 99. Superiority. A class action will provide substantial benefits and is superior to all
25 other available means for the fair and efficient adjudication of this controversy. The damages or
26 other financial detriment suffered by individual Class Members are relatively small compared to
27

1 the burden and expense that individual litigation against Defendant would require. Thus, it would
2 be practically impossible for Class Members, on an individual basis, to obtain effective redress
3 for their injuries. Not only would individualized litigation increase the delay and expense to all
4 parties and the courts, but individualized litigation would also create the danger of inconsistent or
5 contradictory judgments arising from the same set of facts. By contrast, the class action device
6 provides the benefits of adjudication of these issues in a single proceeding, ensures economies of
7 scale, provides comprehensive supervision by a single court, and presents no unusual
8 management difficulties.

9 **FIRST CAUSE OF ACTION**
10 **Negligence**
11 **(On Behalf of Plaintiffs and the Class)**

12 100. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

13 101. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with
14 the understanding that Defendant would safeguard their PII, use their PII for business purposes
15 only, and/or not disclose their PII to unauthorized third parties.

16 102. Defendant owed a duty of care to Plaintiffs and Class Members because it was
17 foreseeable that Defendant's failure—to use adequate data security in accordance with industry
18 standards for data security—would compromise their PII in a data breach. And here, that
19 foreseeable danger came to pass.

20 103. Defendant has full knowledge of the sensitivity of the PII and the types of harm
21 that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

22 104. Defendant owed these duties to Plaintiffs and Class Members because they are
23 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew
24 or should have known would suffer injury-in-fact from Defendant's inadequate security practices.
25 After all, Defendant actively sought and obtained Plaintiffs and Class Members' PII.

26 105. Defendant owed—to Plaintiffs and Class Members—at least the following duties
27 to:

- 1 a. exercise reasonable care in handling and using the PII in their care and
- 2 custody;
- 3 b. implement industry-standard security procedures sufficient to reasonably
- 4 protect the information from a data breach, theft, and unauthorized;
- 5 c. promptly detect attempts at unauthorized access;
- 6 d. notify Plaintiffs and Class Members within a reasonable timeframe of any
- 7 breach to the security of their PII.

8 106. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and
9 Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is
10 required and necessary for Plaintiffs and Class Members to take appropriate measures to protect
11 their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps
12 to mitigate the harm caused by the Data Breach.

13 107. Defendant also had a duty to exercise appropriate clearinghouse practices to
14 remove PII it was no longer required to retain under applicable regulations.

15 108. Defendant knew or reasonably should have known that the failure to exercise due
16 care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an
17 unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the
18 criminal acts of a third party.

19 109. Defendant's duty to use reasonable security measures arose because of the special
20 relationship that existed between Defendant and Plaintiffs and the Class. That special relationship
21 arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary
22 part of obtaining services from Defendant.

23 110. The risk that unauthorized persons would attempt to gain access to the PII and
24 misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that
25 unauthorized individuals would attempt to access Defendant's databases containing the PII —
26 whether by malware or otherwise.

1 111. PII is highly valuable, and Defendant knew, or should have known, the risk in
2 obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class Members' and the
3 importance of exercising reasonable care in handling it.

4 112. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the
5 Class in deviation of standard industry rules, regulations, and practices at the time of the Data
6 Breach.

7 113. Defendant breached these duties as evidenced by the Data Breach.

8 114. Defendant acted with wanton and reckless disregard for the security and
9 confidentiality of Plaintiffs' and Class Members' PII by:

- 10 a. disclosing and providing access to this information to third parties and
11 b. failing to properly supervise both the way the PII was stored, used, and
12 exchanged, and those in their employ who were responsible for making
13 that happen.

14 115. Defendant breached its duties by failing to exercise reasonable care in supervising
15 their agents, contractors, vendors, and suppliers, and in handling and securing the personal
16 information and PII of Plaintiffs and Class Members which actually and proximately caused the
17 Data Breach and Plaintiffs and Class Members' injury.

18 116. Defendant further breached its duties by failing to provide reasonably timely
19 notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused
20 and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' injuries-in-
21 fact.

22 117. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost
23 and disclosed to unauthorized third persons because of the Data Breach.

24 118. As a direct and traceable result of Defendant's negligence and/or negligent
25 supervision, Plaintiffs and Class Members have suffered or will suffer damages, including
26
27

1 monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and
2 emotional distress.

3 119. And, on information and belief, Plaintiffs’ PII has already been published—or
4 will be published imminently—by cybercriminals on the Dark Web.

5 120. Defendant’s breach of its common-law duties to exercise reasonable care and its
6 failures and negligence actually and proximately caused Plaintiffs and Class Members actual,
7 tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by
8 criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and
9 lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted
10 from and were caused by Defendant’s negligence, which injury-in-fact and damages are ongoing,
11 imminent, immediate, and which they continue to face.

12
13 **SECOND CAUSE OF ACTION**
14 **Negligence *per se***
15 **(On Behalf of Plaintiffs and the Class)**

16 121. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

17 122. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate
18 computer systems and data security practices to safeguard Plaintiffs’ and Class Members’ PII.

19 123. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,”
20 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such
21 as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC
22 publications and orders promulgated pursuant to the FTC Act also form part of the basis of
23 Defendant’s duty to protect Plaintiffs and the Class Members’ sensitive PII.

24 124. Defendant breached its respective duties to Plaintiffs and Class Members under
25 the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security
26 practices to safeguard PII.

27 125. Defendant violated its duty under Section 5 of the FTC Act by failing to use
28 reasonable measures to protect PII and not complying with applicable industry standards as

1 described in detail herein. Defendant’s conduct was particularly unreasonable given the nature
2 and amount of PII Defendant had collected and stored and the foreseeable consequences of a data
3 breach, including, specifically, the immense damages that would result to individuals in the event
4 of a breach, which ultimately came to pass.

5 126. The harm that has occurred is the type of harm the FTC Act is intended to guard
6 against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,
7 because of its failure to employ reasonable data security measures and avoid unfair and deceptive
8 practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

9 127. But for Defendant’s wrongful and negligent breach of its duties owed, Plaintiffs
10 and Class Members would not have been injured.

11 128. The injury and harm suffered by Plaintiffs and Class Members was the reasonably
12 foreseeable result of Defendant’s breach of its duties. Defendant knew or should have known that
13 Defendant were failing to meet its duties and that its breach would cause Plaintiffs and members
14 of the Class to suffer the foreseeable harms associated with the exposure of their PII.

15 129. Defendant’s various violations and its failure to comply with applicable laws and
16 regulations constitutes negligence *per se*.

17 130. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiffs and
18 Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

19
20 **THIRD CAUSE OF ACTION**
21 **Breach of Implied Contract**
22 **(On Behalf of Plaintiffs and the Class)**

23 131. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

24 132. Plaintiffs and Class Members were required to provide their PII to Defendant as a
25 condition of receiving services provided by Defendant. Plaintiffs and Class Members provided
26 their PII to Defendant in exchange for Defendant’s services.

27 133. Plaintiffs and Class Members reasonably understood that a portion of their
28 payments would be used to pay for adequate cybersecurity measures.

1 134. Plaintiffs and Class Members reasonably understood that Defendant would use
2 adequate cybersecurity measures to protect the PII that they were required to provide based on
3 Defendant's duties under state and federal law and its internal policies.

4 135. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their
5 PII to Defendant in exchange for services.

6 136. In turn, and through internal policies, Defendant agreed to protect and not disclose
7 the PII to unauthorized persons.

8 137. In its Privacy Policy, Defendant represented that it had a legal duty to protect
9 Plaintiffs' and Class Member's PII.

10 138. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and
11 Class Members with prompt and adequate notice of all unauthorized access and/or theft of their
12 PII.

13 139. After all, Plaintiffs and Class Members would not have entrusted their PII to
14 Defendant in the absence of such an agreement with Defendant.

15 140. Plaintiffs and the Class fully performed their obligations under the implied
16 contracts with Defendant.

17 141. The covenant of good faith and fair dealing is an element of every contract. Thus,
18 parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair
19 dealing, in connection with executing contracts and discharging performance and other duties
20 according to its terms, means preserving the spirit—and not merely the letter—of the bargain. In
21 short, the parties to a contract are mutually obligated to comply with the substance of their contract
22 in addition to its form.

23 142. Subterfuge and evasion violate the duty of good faith in performance even when
24 an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And
25 fair dealing may require more than honesty.

1 143. Defendant materially breached the contracts it entered with Plaintiffs and Class
2 Members by:

- 3 a. failing to safeguard their information;
- 4 b. failing to notify them promptly of the intrusion into their computer systems
5 that compromised such information.
- 6 c. failing to comply with industry standards;
- 7 d. failing to comply with the legal obligations necessarily incorporated into
8 the agreements; and
- 9 e. failing to ensure the confidentiality and integrity of the electronic PII that
10 Defendant created, received, maintained, and transmitted.

11 144. In these and other ways, Defendant violated their duty of good faith and fair
12 dealing.

13 145. Defendant’s material breaches were the direct and proximate cause of Plaintiffs’
14 and Class Members’ injuries (as detailed *supra*).

15 146. And, on information and belief, Plaintiffs’ PII has already been published—or will
16 be published imminently—by cybercriminals on the Dark Web.

17 147. Plaintiffs and Class Members performed as required under the relevant
18 agreements, or such performance was waived by Defendant’s conduct.

19
20 **FOURTH CAUSE OF ACTION**
21 **Breach of the Implied Covenant of Good Faith and Fair Dealing**
22 **(On Behalf of Plaintiffs and the Class)**

23 148. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

24 149. Under California law, every contract imposes on each party a duty of good faith
25 and fair dealing in each performance and their enforcement. Thus, parties must act with honesty
26 in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with
27 executing contracts and discharging performance and other duties according to their terms, means

1 preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract
2 are mutually obligated to comply with the substance of their contract in addition to their form.

3 150. Subterfuge and evasion violate the duty of good faith in performance even when
4 an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And
5 fair dealing may require more than honesty.

6 151. Here, Plaintiffs and Defendant entered into a contract (implied in law, fact, or
7 otherwise) whereby Defendant agreed to:

- 8 a. use a portion of the funds generated by Plaintiffs' and Class Members'
9 payments to pay for adequate cybersecurity measures;
- 10 b. use adequate cybersecurity measures as required by state law, federal law,
11 and Defendant's contractual agreements (implied or otherwise); and
- 12 c. notify them promptly of any exposure of their PII.

13 152. As current and former customers, Plaintiffs and Class Members fully fulfilled their
14 contractual obligations when they provided their PII to Defendant.

15 153. Furthermore, the conditions precedent (if any) to Defendant's performance have
16 already occurred.

17 154. Defendant unfairly interfered with the Plaintiffs' and Class Members' rights to
18 receive the benefits of the contract—and breached the covenant of good faith and fair dealing—
19 by, *inter alia*:

- 20 a. failing to safeguard their information;
- 21 b. failing to notify them promptly of the intrusion into their computer systems
22 that compromised such information.
- 23 c. failing to comply with industry standards;
- 24 d. failing to comply with their legal obligations; and
- 25 e. failing to ensure the confidentiality and integrity of the electronic PII that
26 Defendant created, received, maintained, and transmitted.

1 155. Defendant’s material breaches were the direct and proximate cause of Plaintiffs’
2 and Class Members’ injuries (as detailed *supra*).

3
4 **FIFTH CAUSE OF ACTION**
5 **Unjust Enrichment**
6 **(On Behalf of Plaintiffs and the Class)**

7 156. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

8 157. This claim is pleaded in the alternative to the breach of implied contract claim.

9 158. Plaintiffs and Class Members conferred a benefit upon Defendant. After all,
10 Defendant benefitted from (1) using their PII to provide services, and (2) their payments.

11 159. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs
12 and Class Members.

13 160. Plaintiffs and Class Members reasonably understood that Defendant would use
14 adequate cybersecurity measures to protect the PII that they were required to provide based on
15 Defendant’s duties under state and federal law and its internal policies.

16 161. Defendant enriched itself by saving the costs it reasonably should have expended
17 on data security measures to secure Plaintiffs’ and Class Members’ PII.

18 162. Instead of providing a reasonable level of security, or retention policies, that would
19 have prevented the Data Breach, Defendant instead calculated to avoid its data security
20 obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective
21 security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and
22 proximate result of Defendant’s failure to provide the requisite security.

23 163. Under principles of equity and good conscience, Defendant should not be
24 permitted to retain the full value of Plaintiffs’ and Class Members’ (1) PII and (2) their payments
25 because Defendant failed to adequately protect their PII.

26 164. Plaintiffs and Class Members have no adequate remedy at law.
27

1 165. Defendant should be compelled to disgorge into a common fund—for the benefit
2 of Plaintiffs and Class Members—all unlawful or inequitable proceeds that they received because
3 of its misconduct.

4 **SIXTH CAUSE OF ACTION**
5 **Violation of California’s Unfair Competition Law (UCL)**
6 **Cal. Bus. & Prof. Code § 17200, *et seq.***
7 **(On Behalf of Plaintiffs and the Class)**

8 166. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

9 167. Defendant engaged in unlawful and unfair business practices in violation of Cal.
10 Bus. & Prof. Code § 17200, *et seq.* which prohibits unlawful, unfair, or fraudulent business acts
11 or practices (“UCL”).

12 168. Defendant’s conduct is unlawful because it violates the California Consumer
13 Privacy Act of 2018, Civ. Code § 1798.100, *et seq.* (the “CCPA”) and the California Customer
14 Records Act, Cal. Civ. Code § 1798.80, *et seq.* (the “CRA”), and other state data security laws.

15 169. Defendant stored the PII of Plaintiffs and the Class in its computer systems and
16 knew or should have known that they did not employ reasonable, industry standard, and
17 appropriate security measures that complied with applicable regulations and that would have kept
18 Plaintiffs’ and the Class’s PII secure to prevent the loss or misuse of that PII.

19 170. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure.
20 However, Plaintiffs and the Class were entitled to assume, and did assume, that Defendant had
21 secured their PII. At no time were Plaintiffs and the Class on notice that their PII was not secure,
22 which Defendant had a duty to disclose.

23 171. Defendant also violated California Civil Code § 1798.150 by failing to implement
24 and maintain reasonable security procedures and practices, resulting in an unauthorized access
25 and exfiltration, theft, or disclosure of Plaintiffs’ and the Class’s nonencrypted and nonredacted
26 PII.

27 172. Had Defendant complied with these requirements, Plaintiffs and the Class would
28 not have suffered the damages related to the data breach.

1 173. Defendant’s conduct was unlawful, in that they violated the CCPA.

2 174. Defendant’s acts, omissions, and misrepresentations as alleged herein were
3 unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

4 175. Defendant’s conduct was also unfair, in that it violated a clear legislative policy in
5 favor of protecting consumers from data breaches.

6 176. Defendant’s conduct is an unfair business practice under the UCL because it was
7 immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct
8 includes employing unreasonable and inadequate data security despite its business model of
9 actively collecting PII.

10 177. Defendant also engaged in unfair business practices under the “tethering test.” Its
11 actions and omissions, as described above, violated fundamental public policies expressed by the
12 California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all
13 individuals have a right of privacy in information pertaining to them . . . The increasing use of
14 computers . . . has greatly magnified the potential risk to individual privacy that can occur from
15 the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the
16 Legislature to ensure that personal information about California residents is protected.”); Cal.
17 Bus. & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the
18 Online Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and
19 omissions thus amount to a violation of the law.

20 178. Instead, Defendant made the PII of Plaintiffs and the Class accessible to scammers,
21 identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending
22 risk of identity theft. Additionally, Defendant’s conduct was unfair under the UCL because it
23 violated the policies underlying the laws set out in the prior paragraph.

24 179. As a result of those unlawful and unfair business practices, Plaintiffs and the Class
25 suffered an injury-in-fact and have lost money or property.

1 180. For one, on information and belief, Plaintiffs’ and the Class’s stolen PII has
2 already been published—or will be published imminently—by cybercriminals on the dark web.

3 181. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing
4 benefit to consumers or competition under all of the circumstances.

5 182. There were reasonably available alternatives to further Defendant’s legitimate
6 business interests, other than the misconduct alleged in this complaint.

7 183. Therefore, Plaintiffs and the Class are entitled to equitable relief, including
8 restitution of all monies received by Defendant; disgorgement of all profits accruing to Defendant
9 because of its unfair and improper business practices; a permanent injunction enjoining
10 Defendant’s unlawful and unfair business activities; and any other equitable relief the Court
11 deems proper.

12 **SEVENTH CAUSE OF ACTION**
13 **Violations of the California Consumer Privacy Act (“CCPA”)**
14 **Cal. Civ. Code § 1798.150**
15 **(On Behalf of Plaintiffs and the Class)**

16 184. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

17 185. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to
18 implement and maintain reasonable security procedures and practices appropriate to the nature of
19 the information to protect the nonencrypted PII of Plaintiffs and the Class. As a direct and
20 proximate result, Plaintiffs’ and the Class’s nonencrypted and nonredacted PII was subject to
unauthorized access and exfiltration, theft, or disclosure.

21 186. Defendant are each a “business” under the meaning of Civil Code § 1798.140
22 because Defendant are each a “corporation, association, or other legal entity that is organized or
23 operated for the profit or financial benefit of its shareholders or other owners” that “collects
24 consumers’ personal information” and is active “in the State of California” and “had annual gross
25 revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year.”
26 Civil Code § 1798.140(d).

1 187. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure
2 Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures
3 and practices. Such relief is particularly important because Defendant continue to hold PII,
4 including Plaintiffs' and Class Members' PII. Plaintiffs and Class Members have an interest in
5 ensuring that their PII is reasonably protected, and Defendant have demonstrated a pattern of
6 failing to adequately safeguard this information.

7 188. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice
8 letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that
9 Defendant have violated and continues to violate. If Defendant cannot cure within 30 days—and
10 Plaintiffs believe such cure is not possible under these facts and circumstances—then Plaintiffs
11 intend to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

12 189. As described herein, an actual controversy has arisen and now exists as to whether
13 Defendant implemented and maintained reasonable security procedures and practices appropriate
14 to the nature of the information so as to protect the personal information under the CCPA.

15 190. A judicial determination of this issue is necessary and appropriate at this time
16 under the circumstances to prevent further data breaches by Defendant.

17
18 **EIGHTH CAUSE OF ACTION**
19 **Declaratory Judgment**
(On Behalf of Plaintiffs and the Class)

20 191. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

21 192. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
22 authorized to enter a judgment declaring the rights and legal relations of the parties and to grant
23 further necessary relief. The Court has broad authority to restrain acts, such as those alleged
24 herein, which are tortious and unlawful.

25 193. In the fallout of the Data Breach, an actual controversy has arisen about
26 Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs
27

1 allege that Defendant’s actions were—and *still* are—inadequate and unreasonable. And Plaintiffs
2 and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

3 194. Given its authority under the Declaratory Judgment Act, this Court should enter a
4 judgment declaring, among other things, the following:

- 5 a. Defendant owed—and continue to owe—a legal duty to use reasonable
6 data security to secure the data entrusted to it;
- 7 b. Defendant have a duty to notify impacted individuals of the Data Breach
8 under the common law and Section 5 of the FTC Act;
- 9 c. Defendant breached, and continue to breach, its duties by failing to use
10 reasonable measures to the data entrusted to it; and
- 11 d. Defendant’s breach of its duties caused—and continue to cause—injuries
12 to Plaintiffs and Class Members.

13 195. The Court should also issue corresponding injunctive relief requiring Defendant
14 to use adequate security consistent with industry standards to protect the data entrusted to it.

15 196. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury
16 and lack an adequate legal remedy if Defendant experience a second data breach.

17 197. And if a second breach occurs, Plaintiffs and the Class will lack an adequate
18 remedy at law because many of the resulting injuries are not readily quantified in full and they
19 will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary
20 damages—while warranted for out-of-pocket damages and other legally quantifiable and provable
21 damages—cannot cover the full extent of Plaintiffs and Class Members’ injuries.

22 198. If an injunction is not issued, the resulting hardship to Plaintiffs and Class
23 Members far exceeds the minimal hardship that Defendant could experience if an injunction is
24 issued.

25 199. An injunction would benefit the public by preventing another data breach—thus
26 preventing further injuries to Plaintiffs, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;
- D. Enjoining Defendant from further unfair and/or deceptive practices;
- E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: April 3, 2026

Respectfully submitted,

By: /s/ Carly M. Roman

Carly M. Roman (No. 349895)

croman@straussborrelli.com

STRAUSS BORRELLI PLLC

980 N. Michigan Ave., Suite 1610

Chicago, IL 60611

2261 Market St., Ste. 22946

San Francisco, CA 94114

Telephone: (872) 263-1100

Facsimile: (872) 263-1109

Attorneys for Plaintiff and Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Chime Data Breach Lawsuit Says April 2026 Incident Could Have Been Prevented](#)
