Kristin J. Moody (SBN 206326)
Pierce H. Stanley (SBN 352152)
BERMAN TABACCO
425 California Street, Suite 2300
San Francisco, CA 94104
Telephone: (415) 433-3200
Email: kmoody@bermantabacco.com
pstanley@bermantabacco.com

Patrick T. Egan (*pro hac vice* forthcoming)
BERMAN TABACCO
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
Email: pegan@bermantabacco.com

Counsel for Plaintiffs Mildred Kinchen and James Kinchen and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MILDRED KINCHEN and JAMES KINCHEN, individually and on behalf of all others similarly situated, Plaintiffs, v. AT&T MOBILITY LLC and AT&T INC., Defendants.	Civil Action No.: **CLASS ACTION COMPLAINT** **CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs Mildred Kinchen and James Kinchen ("Plaintiffs"), individually and on behalf of themselves and all others similarly situated, allege the following against AT&T Mobility LLC and AT&T Inc. (collectively, "AT&T" or "Defendants"). The following allegations are based upon Plaintiffs' personal knowledge with respect to themselves and their own acts, and on information and belief as to all other matters.

I. INTRODUCTION

1. Plaintiffs and Class Members bring this class action against AT&T for its failures to properly secure and safeguard Plaintiffs' and similarly situated individuals' private and confidential information, including but not limited to names, mailing addresses, telephone

numbers, dates of birth, Social Security numbers, usernames, account numbers, PIN numbers, and passwords ("Personal Information").

2. AT&T Inc. is a multinational telecommunications company that markets a range of consumer products including internet, telephone, and wireless services. AT&T Mobility LLC is a wholly owned subsidiary of AT&T Inc. that provides wireless and cellular services in the United States. AT&T Mobility LLC is the largest wireless carrier in the United States, with over 241.5 million subscribers.[1]

3. This class action is brought on behalf of all citizens of all states in the United States who are the victims of a targeted cyberattack on Defendants that occurred on or around March 17, 2024 (the "Data Breach").

4. In 2019, AT&T learned that a well-known threat actor claimed to be selling a database containing the Personal Information of over 73 million AT&T customers. This Personal Information included customers' names, addresses, phone numbers, Social Security numbers, passcodes, and dates of birth, among other information. Instead of investigating the cause of this massive data breach at the time, AT&T denied the allegations, ignored the issue, and continued with its operations.

5. In August 2021, the threat actor resurfaced with the claim to have stolen millions of AT&T customers' data, publishing a small sample of the leaked records online. When questioned at the time, AT&T turned a blind eye to pending disaster, saying that the leaked data "does not appear to have come from our systems," and AT&T chose not to speculate as to where the data had originated or whether it was valid.[2]

[1] AT&T Inc., Current Report (Form 8-K) (Jan. 24, 2024), https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2023/4q-2023/ATT_4Q_2023_8_K_Earnings_8_01.pdf.

[2] Lawrence Abrams, *AT&T denies data breach after hacker auctions 70 million user database*, BLEEPINGCOMPUTER (Aug. 20, 2021), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/.

6. Only when, three years later, the contents of the database were publicly leaked on the dark web and independently verified, did AT&T admit the breach occurred and, purportedly, began an investigation.

7. It took until March 2024, when an online data seller published the full 73 million alleged AT&T records on a known cybercrime forum—allowing for a detailed analysis of the leaked records—for AT&T to admit the authenticity of the breached records.[3] At this point, AT&T reset the passcodes of at least 7.6 million existing customers and notified all current and former customers whose Personal Information was compromised.[4]

8. On April 10, 2024, AT&T began notifying U.S. state authorities and privacy regulators that a security incident had occurred, and Defendants confirmed that the millions of customer records that were posted online by threat actors in March 2024 were indeed authentic.[5] Notices sent directly to Plaintiffs and other Class Members and notices sent to state attorneys general offices will be collectively referred to as "Notice."

9. On April 11, 2024, AT&T began mailing Notice of the data security incident to Plaintiffs and other Class Members. According to the Notice, entitled "Important Information," AT&T wrote that "after a thorough assessment, AT&T has determined that "some of [Plaintiffs'] personal information was compromised."[6]

10. As a result of Defendants' inability to properly secure Plaintiffs' and the Class Members' private Personal Information, data thieves were able to access and obtain the Personal Information of Plaintiffs and Class Members as early as 2019. For nearly five years, AT&T had knowledge of this threat and did not meaningfully act upon it until it publicly announced the

[3] Zack Whittaker, *AT&T resets account passcodes after millions of customer records leak online*, TECHCRUNCH (Mar. 30, 2024), https://techcrunch.com/2024/03/30/att-reset-account-passcodes-customer-data/.

[4] *Id.*

[5] Zack Whittaker, *AT&T notifies regulators after customer data breach*, TECHCRUNCH (Apr. 10, 2024), https://techcrunch.com/2024/04/10/att-notifies-regulators-after-customer-data-breach.

[6] Data Breach Notice Letter to Customers, *Important Information*, AT&T Inc. (Apr. 11, 2024).

veracity of the threat actor's claims in March 2024 and told individual customers about the vulnerability as late as mid-April 2024.

11. The Notice failed to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the Class Members' Personal Information, what AT&T product contained the vulnerability, and whether the breach was a system-wide breach or was limited to a certain subset of customers.

12. The Notice also failed to provide details on how many people were impacted by the Data Breach. In an April 10, 2024 filing with the Maine Attorney General's Office, AT&T stated that the Data Breach affected 51.2 million people.[7]

13. Defendants knowingly collected the Personal Information of customers in confidence, and thus, have a resulting duty to secure, maintain, protect, and safeguard that Personal Information against unauthorized access and disclosure through reasonable and adequate security measures.

14. As a result of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses, including, but not limited to, a loss of potential value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendants, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

15. Plaintiffs and Class Members entrusted their Personal Information to Defendants, their officials, and agents. That Personal Information was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

16. Plaintiffs bring this class action lawsuit on behalf of themselves and all others similarly situated to address Defendants' inadequate safeguarding of Plaintiffs' and Class Members' Personal Information, for failing to provide adequate notice to Plaintiffs and other Class Members of the unauthorized access to their Personal Information by a cyber attacker, and

[7] Office of Att'y Gen. of Maine, *Data Breach Notifications*, AT&T Inc. (Apr. 10, 2024), https://apps.web.maine.gov/online/aeviewer/ME/40/3778e1fc-2ed5-461d-9cc5-df15c07f687c.shtml.

for failing to provide adequate and timely notice of precisely what information was accessed and stolen.

17. Defendants breached their duties to Plaintiffs and Class Members by maintaining Plaintiffs' and the Class Members' Personal Information in a negligent and reckless manner.

18. Upon information and belief, the means of the Data Breach and potential risk for improper disclosure of Plaintiffs' and Class Members' Personal Information were known and foreseeable to Defendants. Thus, Defendants were on notice that failing to take steps necessary to secure the Personal Information from those risks and left the Personal Information in a dangerous and vulnerable condition for an extended period of time.

19. Defendants failed to properly monitor the computer network and systems housing the Personal Information.

20. Had Defendants properly monitored their property, they would have discovered the intrusion sooner or been able to wholly prevent it, or when having known of the possibility of an intrusion years ago, acted expeditiously to remedy it.

21. Exacerbating an already devastating privacy intrusion, Plaintiffs' and Class Members' identities are now at a heightened risk of exposure because of Defendants' negligent conduct since the Personal Information that Defendants collected and stored is now in the hands of data thieves and cybercriminals.

22. Armed with the Personal Information accessed in the Data Breach, data thieves can now use the Personal Information obtained from Defendants to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

23. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered fraud and will continue to be exposed to a heightened and imminent risk of fraud and identity

theft, potentially for the rest of their lives. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

24. Plaintiffs and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

25. As a direct and proximate result of the Data Breach and subsequent exposure of their Personal Information, Plaintiffs and Class Members have suffered, and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam phone calls, letters, and emails received as a result of the Data Breach.

26. Plaintiffs and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own Personal Information such that they are entitled to damages from Defendants for unauthorized access to, theft of, and misuse of their Personal Information.

27. These harms are ongoing, and Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Personal Information as thieves will continue to use the information to obtain money and credit in their names for several years.

28. Plaintiffs seek to remedy these harms on behalf of all similarly situated individuals whose Personal Information was accessed via and/or compromised by AT&T during the Data Breach.

29. Accordingly, Plaintiffs bring this action on behalf of themselves and all others similarly situated against Defendants, seeking redress for Defendants' unlawful conduct asserting claims for (I) negligence; (II) negligence *per se*; (III) breach of implied contract; (IV) unjust enrichment; (V) violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*; (VI) violation of California's Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150, *et seq.*; and (VII) declaratory judgment seeking damages and injunctive relief.

II. PARTIES

A. Plaintiffs

30. Plaintiffs Mildred Kinchen and James Kinchen are residents of Elk Grove, California and citizens of California.

31. Mildred Kinchen is a current AT&T customer, and James Kinchen has previously been an AT&T customer.

B. Defendants

32. Defendant AT&T Mobility LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia.

33. Defendant AT&T Inc. is a Delaware corporation with its principal place of business in Dallas, Texas.

III. JURISDICTION AND VENUE

34. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs, is a citizen of a state different from Defendants.

35. This Court has personal jurisdiction over Defendants because Defendants have committed acts within this District giving rise to this action and established minimum contacts with this District such that the exercise of jurisdiction over Defendants would not offend traditional notions of fairly play and substantial justice. Defendants purposefully availed themselves of the laws, rights, and benefits of the State of California by engaging in activities including (i) directly and/or through its parent companies, affiliates, and/or agents providing services throughout the United States in this District; (ii) conducting substantial business in this District; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in California and in this judicial District. Moreover, Defendants have engaged in continuous, systematic, and substantial activities within this State, including

marketing and sales of services and products in connection with the customers impacted by the Data Breach in this State.

36. Venue is proper under 28 U.S.C § 1391(b)(2) because a substantial part of the events and omissions giving rise to this action occurred in this District, including unknown actors copying and exfiltrating the Personal Information of AT&T's customers, causing harm to Plaintiffs and Class Members in this District.

37. Divisional Assignment: Assignment to the San Francisco Division of this District is proper pursuant to Northern District of California Civil Local Rule 3-5(b) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in San Francisco County, and under Civil Local Rule 3-2(c), all civil actions which arise in San Francisco County shall be assigned to the San Francisco Division.

IV. FACTUAL ALLEGATIONS

A. Defendant AT&T's Business

38. AT&T is an American telecommunications business that markets a range of consumer products including internet, telephone, cellular, and wireless communications services.

39. AT&T is one of the largest wireless carriers and internet providers in the country with 241.5 million subscribers at the end of 2023.

40. Plaintiffs and Class Members are current and former customers of Defendants telecommunications services.

41. Given the amount and sensitive nature of the data it collects in order to provide customers with its services, AT&T maintains privacy policies explaining its privacy practices regarding the security and handling of consumers' Personal Information.

42. AT&T expressly assumes these duties in its Privacy Policy posted on the company website, stating, "[AT&T] work[s] hard to safeguard [customers'] information using technology controls and organizational controls."[8]

[8] *AT&T Privacy Notice*, AT&T Inc. (eff. Dec. 11, 2023), https://about.att.com/privacy/privacy-notice.html (last accessed Apr. 23, 2024).

43. In addition, AT&T further states that it "limit[s] access to [P]ersonal [I]nformation to the people who need access for their jobs."[9] AT&T further warrants that when customers' Personal Information is no longer needed, that it will "destroy it by making it unreadable or indecipherable,"[10] and that in the event of a data breach incident, AT&T will "notify [customers] as required by law."[11]

44. Given AT&T's experience handling high volumes of highly sensitive Personal Information, it understood the need to protect consumers' personal and Personal Information and knew that effective data security practices and timely notice were paramount.

B. The Collection of Plaintiffs' and Class Members' Personal Information is Central to Defendants' Businesses

45. In exchange for providing Plaintiffs and Class Members telecommunications services, Plaintiffs and Class Members were required to transfer possession of their Personal Information to Defendants.

46. Through the possession and use of Plaintiffs' and Class Members' Personal Information, Defendants assumed duties owed to Plaintiffs and Class Members regarding their Personal Information.

47. Therefore, Defendants knew or should have known that they were responsible for safeguarding Plaintiffs' and Class Members' Personal Information from unauthorized access and criminal misuse.

48. Plaintiffs and Class Members relied on Defendants to keep their Personal Information secure and safeguarded for authorized purposes. Defendants owed a duty to Plaintiffs to secure their Personal Information as such, and ultimately Defendants breached that duty.

---

[9] *Id.*

[10] *Id.*

[11] *Id.*

C. The Data Breach

49. On or around March 17, 2024, the details of 73 million former and current AT&T customer accounts, including full names, email addresses, mailing addresses, phone numbers, dates of birth, Social Security numbers, AT&T account numbers, PIN numbers, and passcodes were leaked online.[12] In response to the revelation, AT&T reset the passcodes of millions of affected customers.

50. Details of the leaked data first appeared online in August 2021 when a well-known threat actor, ShinyHunters, with a long history of compromising websites and developer repositories to steal credentials, "began selling th[e] database … on a hacking forum with a starting price of $200,000 and incremental offers of $30,000. The hacker state[d] that they [were] willing to sell it immediately for $1 million."[13]

51. Upon learning of ShinyHunters's claims, AT&T denied that the data came from its servers. When pressed about whether the information could have been stolen from a third-party partner or breached by some other means, AT&T stated that it could not "speculate on where [the data] came from or whether it [was] valid."[14]

52. AT&T continued to deny responsibility for weeks even after independent security researchers confirmed that some of the dataset samples related to persons with AT&T accounts.[15] Samples taken from the dataset at the time of auction by the threat actor showed that the database contained customer names, addresses, phone numbers, Social Security numbers, and dates of birth.[16]

[12] Aimee Ortiz, *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, N.Y. TIMES (Mar. 30, 2024), https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html.

[13] Abrams, *supra* n. 2.

[14] *Id.*

[15] *Id.*

[16] *Id.*

53. In March 2024, that same data appeared to have been made available online for free in a hacking forum by another well-known threat actor, MajorNelson,[17] at which point AT&T finally acknowledged the legitimacy of the leaked customer data, posting publicly on its website, "AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago."[18]

54. Following Defendants' realization and public acknowledgement of the Data Breach, AT&T failed to provide meaningful Notice to Plaintiffs and the Class Members.

55. Any Notice provided by Defendants failed to include substantive details on the extent of the Data Breach, the software and/or programs exploited in the Data Breach, what subset of customers had what information stolen in the Data Breach, and what steps were taken to mitigate the risk of subsequent cyberattacks and further harm to Plaintiffs and the Class Members.

56. Further, in their acknowledgment of the Data Breach, AT&T failed to address the alleged AT&T database that was originally offered for sale in 2021 and published on the dark web for free almost three years later. Within the intervening years, AT&T failed to adequately determine whether its systems were impacted, whether the data originated from AT&T or third-party servers, and by doing so, AT&T failed to protect customers from continued or future intrusions.

D. Plaintiffs Mildred Kinchen and James Kinchen's Experiences Following the Data Breach

57. Plaintiffs Mildred Kinchen and James Kinchen are currently or have been customers of AT&T. Specifically, they are or have been wireless cellular telephone customers and use or have used their AT&T cellular telephone accounts for personal purposes.

[17] Ernestas Naprys, *Hacker gives out 70 million stolen AT&T user records*, CYBERNEWS (updated Mar. 18, 2024), https://cybernews.com/news/hacker-gives-out-stolen-att-records/.

[18] AT&T News, *AT&T Addresses Recent Data Set Released on the Dark Web*, AT&T Inc. (Mar. 30, 2024), https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html.

58. Plaintiff Mildred Kinchen is a current AT&T customer and currently maintains an active AT&T wireless cellular telephone service account.

59. Plaintiff James Kinchen is a previous AT&T customer and former wireless cellular telephone service account holder.

60. Plaintiffs were required to provide AT&T with their Personal Information as a condition of receiving telecommunications services.

61. Plaintiffs received Notice of the Data Breach from AT&T by logging into their account in March 2024. Upon logging in, Plaintiffs saw the alert that AT&T had experienced the Data Breach, and they responded to a prompt that urged them to change their password and set up two-factor authentication.[19]

62. Plaintiff Mildred Kinchen received Notice of the Data Breach from AT&T in a letter emailed to her on April 11, 2024.

63. Plaintiff James Kinchen received Notice of the Data Breach from AT&T in a letter emailed to him on April 18, 2024.

64. Thereafter, Plaintiffs spent time taking action to mitigate the impact of the Data Breach. This effort included checking their bank accounts and other online accounts, changing their passwords, examining their credit score, and researching the potential impact of the Data Breach, all as a result of their Personal Information being exposed in the Data Breach.

65. Plaintiffs intend to spend additional time and effort taking steps to protect their Personal Information in the future. Because of the Data Breach, Plaintiffs spent valuable time attempting to mitigate the harm they otherwise would have spent on other obligations.

66. Moreover, Plaintiffs spent this time at Defendant AT&T's direction. In the Notice posted by AT&T, AT&T encouraged Plaintiffs and Class Members to spend time mitigating

[19] AT&T Support, *Keeping your account secure*, AT&T Inc., https://www.att.com/support/article/my-account/000101995 (last accessed Apr. 23, 2024).

their losses by creating new passwords.[20] AT&T also stated that Plaintiffs and Class Members should "remain vigilant by monitoring account activity and credit reports."[21]

67. As a result of the Data Breach, Plaintiffs have suffered lost time, annoyance, interference, and inconvenience. This is time Plaintiffs otherwise would have spent performing other activities, such as their job, and/or leisurely activities for the enjoyment of life.

68. As a result of the Data Breach, Plaintiffs have suffered emotional distress because of the release of their Personal Information which they expected Defendants to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing, and potentially using their Personal Information.

69. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for financial fraud, medical fraud, and identity theft, and the attendant damages, for years to come.

E. Defendants Knew or Should Have Known Both the Value of Personal Information and the Risk of Cyberattacks to Those Who Possess Such Personal Information

70. At all relevant times, Defendants were well aware that the Personal Information they collect from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

71. Personal Information is a valuable commodity to cyber attackers. As the U.S. Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[22]

72. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Personal Information on multiple underground websites, commonly referred to as the dark web.

73. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[23] In 2022, 1,802

---

[20] *Id.*

[21] *Id.*

[22] *What to Know About Identify Theft*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Apr. 16, 2024).

[23] Press Release, CyberScout, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017),

data compromises were reported to have impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[24] That upward trend continues.

74. The ramifications of Defendants' failures to keep Plaintiffs' and Class Members' Personal Information secure are long-lasting and severe. Once Personal Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

75. Further, criminals often trade stolen Personal Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Personal Information on the internet, thereby making such information readily and publicly available.

76. Approximately twenty-one percent of victims do not realize their identities have been compromised until more than two years after it has happened. This gives data thieves ample time to seek multiple treatments or pursue multiple financial schemes under the victim's name.

77. As entities serving consumers in the information technology, software, and telecommunications space, Defendants knew, or reasonably should have known, the importance of safeguarding Plaintiffs' and Class Members' Personal Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. Defendants Failed to Comply with FTC Guidelines

78. Defendants were also prohibited by the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and

https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[24] 2022 Annual Data Breach Report, IDENTITY THEFT RES. CTR. (Jan. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf.

appropriate data security for consumers' sensitive personal and Personal Information is an "unfair practice" in violation of the FTCA.[25]

79. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

80. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[27] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Personal Information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.

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

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

[25] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[26] *Start With Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

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

83. Defendants failed to properly implement basic data security practices. Defendants' failures to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

84. Defendants were fully aware of their obligations to protect the Personal Information of Plaintiffs and Class Members because of their positions as entities whose businesses center on contractual relationships with their clients and necessary collection, storage, and safeguarding of Personal Information as a result of those contractual relationships. Defendants were also aware of the significant repercussions that would result from their failures to make good on those obligations.

G. Cybercriminals Have and Will Continue to Use Plaintiffs' and Class Members' Personal Information for Nefarious Purposes

85. Plaintiffs' and Class Members' Personal Information is of great value to cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access Defendants' systems in order to obtain valuable Personal Information to sell on the dark web.

86. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

87. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to personally identifiable information, they will use it.[28]

88. Cyber thieves may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[28] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://web.archive.org/web/20220201130728/https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. [29]

89. If cyber criminals manage to access financial information, health insurance information, and other personally sensitive data using the Personal Information compromised in the Data Breach, there is no limit to the amount of fraud to which Defendants may have exposed the Plaintiffs and Class Members.

H. Plaintiffs and Class Members Suffered Damages

90. The ramifications of Defendants' failures to keep Plaintiffs' and Class Members' Personal Information secure are long lasting and severe. Once Personal Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[30]

91. In addition to their obligations under state laws and regulations, Defendants owed a common law duty to Plaintiffs and Class Members to protect Personal Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

92. Defendants further owed and breached their duties to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

93. As a direct result of Defendants' intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber thieves were able to access, acquire, view,

---

[29] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, Gov. Accountability Office (June 2007), https://www.gao.gov/assets/a262904.html.

[30] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://risk.lexisnexis.com/-/media/files/corporations%20and%20non%20profits/research/true-cost-fraud-2014%20pdf.pdf.

publicize, and/or otherwise cause the misuse and/or identity theft of Plaintiffs' and Class Members' Personal Information as detailed above, and Plaintiffs and Class Members are now at a heightened risk of identity theft and fraud.

94. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

95. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

96. Plaintiffs and Class Members did not receive the full benefit of the bargain for the received telecommunications services. As a result, Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value of the telecommunications services with data security protection they paid for and the services they received without the data security protection.

97. As a result of the Data Breach, Plaintiffs' and Class Members' Personal Information has diminished in value.

98. The Personal Information belonging to Plaintiffs and Class Members is private in nature and was left inadequately protected by Defendants who did not obtain Plaintiffs' or Class Members' consent to disclose such Personal Information to any other person as required by applicable law and industry standards.

99. The Data Breach was a direct and proximate result of Defendants' failures to: (a) properly safeguard and protect Plaintiffs' and Class Members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and

Class Members' Personal Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

100. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligations to protect consumers' data.

101. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of Plaintiffs' and Class Members' Personal Information.

102. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

103. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had [P]ersonal [I]nformation used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[31]

104. Defendants' failures to adequately protect Plaintiffs' and Class Members' Personal Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Rather than assist those affected by the Data Breach, Defendants are putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

[31] Erika Harrell & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS, BUREAU OF JUST. STATS. (Dec. 2013), https://bjs.ojp.gov/content/pub/pdf/vit12.pdf.

105. As a result of Defendants' failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their Personal Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Personal Information in their possession;

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

f. Anxiety and distress resulting from fear of misuse of their Personal Information and loss of privacy.

106. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Personal Information is secure, remains secure, and is not subject to further misappropriation and theft.

V. CLASS ACTION ALLEGATIONS

107. Plaintiffs bring this class action on behalf of themselves and all others similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

108. The Class and Subclass that Plaintiffs seeks to represent are defined as follows, subject to amendment as appropriate:

Nationwide Class

All individuals residing in the United States whose Personal Information was compromised as a result of the Data Breach reported by AT&T in March 2024 (the "Nationwide Class" or "Class").

California Subclass

All individuals residing in California whose Personal Information was compromised as a result of the Data Breach reported by AT&T in March 2024 (the "California Subclass").

109. Collectively, the Class and California Subclass are referred to as the "Classes."

110. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

111. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

112. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all Class Members is impracticable. Defendants have identified at least 73 million individuals whose Personal Information may have been improperly accessed and compromised in the Data Breach.

113. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding, and/or obtaining Class Members' Personal Information;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class Members' Personal Information;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' Personal Information;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' Personal Information secure and prevent loss or misuse of that Personal Information;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiffs' and Class Members' damages;

i. Whether Defendants violated the law by failing to promptly notify Class Members that their Personal Information had been compromised;

j. Whether Plaintiffs and the other Class Members are entitled to actual damages, extended credit monitoring, and other monetary relief; and

k. Whether Defendants violated common law and statutory claims alleged herein.

114. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members, because all had their Personal Information compromised as a result of the Data Breach, due to Defendants' misfeasance.

115. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible

standards of conduct toward the Classes and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' policies challenged herein apply to and affect the Classes uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

116. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

117. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

118. The nature of this action and the nature of laws available to Plaintiffs and the Classes make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Classes for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of the Classes with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered;

proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

119. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

120. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

121. Unless a Class-wide injunction is issued, Plaintiffs and Class Members remain at risk that Defendants will continue to fail to properly secure the Personal Information of Plaintiffs and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

122. Defendants acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Classes as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

a. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, using, and safeguarding their Personal Information;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Personal Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

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

e. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence
(On behalf of Plaintiffs and the Nationwide Class against both Defendants)

124. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

125. Plaintiffs and Class Members were required to submit their Personal Information to Defendants in order to receive telecommunications services.

126. Defendants knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiffs and Class Members.

127. As described above, Defendants owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted with Defendants.

128. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

129. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' Personal Information. Defendants knew or reasonably should have known that they had inadequate data security practices to safeguard such information, and Defendants knew or reasonably should have known that data thieves were attempting to access databases containing personally identifiable information, such as those of Defendants.

130. A "special relationship" exists between Defendants and Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members because Defendants collected the Personal Information of Plaintiffs and the Class Members—information that Plaintiffs and the Class Members were required to provide in order to receive the telecommunications services.

131. But for Defendants' wrongful and negligent breaches of the duties owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

132. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known they were failing to meet their duties, and that Defendants' breaches of such duties would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

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

COUNT II
Negligence *Per Se*
(On behalf of Plaintiffs and the Nationwide Class against both Defendants)

134. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

135. Pursuant to the FTCA, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

136. Defendants breached their duties to Plaintiffs and Class Members under the FTCA, 15 U.S.C. § 45, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

137. Defendants' failures to comply with applicable laws and regulations constitutes negligence *per se*.

138. But for Defendants' wrongful and negligent breaches of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

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

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

COUNT III
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class against both Defendants)

141. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

142. Plaintiffs and Class Members entered into an implied contract with Defendants when they obtained telecommunications services in exchange for which they were required to provide their Personal Information. The Personal Information provided by Plaintiffs and Class Members to Defendants was governed by and subject to Defendants' privacy duties and policies.

143. Defendants agreed to safeguard and protect the Personal Information of Plaintiffs and Class Members and to timely and accurately notify Plaintiffs and Class Members in the event that their Personal Information was breached or otherwise compromised.

144. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

145. Plaintiffs and Class Members would not have entrusted their Personal Information to Defendants in the absence of the implied contract or implied terms between Plaintiffs and

Class Members and Defendants. The safeguarding of the Personal Information of Plaintiffs and Class Members and prompt and sufficient notification of a breach involving Personal Information was critical to realize the intent of the parties.

146. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

147. Defendants breached their implied contracts with Plaintiffs and Class Members to protect Plaintiffs' and Class Members' Personal Information when they: (a) failed to have security protocols and measures in place to protect that information; (b) disclosed that information to unauthorized third parties; and (c) failed to provide sufficient notice that their Personal Information was compromised as a result of the Data Breach.

148. As a direct and proximate result of Defendants' breaches of implied contract, Plaintiffs and Class Members have suffered damages.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Class against both Defendants)

149. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

150. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III).

151. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Personal Information—Personal Information that has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to Defendants' adequate storage and safeguarding of their Personal Information.

152. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members.

153. Defendants profited from Plaintiffs' and Class Members' retained Personal Information and used their Personal Information for business purposes.

154. Defendants failed to store and safeguard Plaintiffs' and Class Members' Personal Information. Thus, Defendants did not fully compensate Plaintiffs and Class Members for the value of their Personal Information.

155. As a result of Defendants' failures, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the services with the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and the inadequate services without reasonable data privacy and security practices and procedures that they received.

156. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to implement—or adequately implement—the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state and local laws, and industry standards.

157. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by Defendants.

158. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiffs and Class Members.

COUNT V
Violation of California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiffs and the California Subclass against both Defendants)

159. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

160. Plaintiffs bring this claim on behalf of themselves and California Subclass Members.

161. The California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

162. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and California Subclass Members' Personal Information, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

163. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the private and confidential Personal Information of consumers has been compromised for all to see, use, or otherwise exploit.

164. Defendants' practices were unlawful and in violation of the FTCA, 15 U.S.C. § 45, as well as violating Cal. Civil Code § 1798, *et seq*. because Defendant failed to take reasonable measures to protect Plaintiffs' and California Subclass Members' Personal Information.

165. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the Personal Information Plaintiffs and California Subclass Members provided to Defendants would remain private and secure, when in fact it was not private and secure.

166. Plaintiffs and California Subclass Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions including, the unauthorized release and disclosure of their Personal Information.

167. Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and California Subclass Members' Personal also constitute "unfair" business acts and practices within the meaning of the UCL, Cal. Bus. & Prof. Code § 17200, *et seq*., in that Defendants' conduct was substantially injurious to Plaintiffs and California Subclass Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous. The gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

168. But for Defendants' misrepresentations and omissions, Plaintiffs and California Subclass Members would not have provided their Personal Information to Defendant or would have insisted that their Personal Information be more securely protected.

169. As a direct and proximate result of Defendants' wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and California Subclass Members' Personal Information, Plaintiffs and California Subclass Members have been injured by: (a) the loss of the opportunity to control how their Personal Information is used; (b) the diminution in the value and/or use of their Personal Information entrusted to Defendants; (c) the compromise, publication, and/or theft of their Personal Information; and (d) costs associated with the monitoring of their Personal Information, among other things.

170. Plaintiffs therefore take upon themselves enforcement of the laws violated by Defendants in connection with the negligent disclosure of Plaintiffs' and California Subclass Members' Personal Information. There is a financial burden incurred in pursuing this action, and it would be against the interests of justice to penalize Plaintiffs by forcing them to pay attorneys' fees and costs from recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate as set forth by California Code of Civil Procedure § 1021.5 and relevant case law.

COUNT VI
Violation of California's Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150, *et seq*.
(On behalf of Plaintiffs and the California Subclass against both Defendants)

171. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

172. Defendants collect consumers' Personal Information, as defined in California by the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.140(v)(1). As a result, Defendants have a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As alleged herein, Defendants failed to do so.

173. AT&T is a corporate enterprise organized for the profit or the commercial and financial benefit of its owners, and, on information and belief, has annual gross revenues

exceeding $25 million and collects Personal Information as defined in the CCPA, Cal. Civ. Code § 1798.140(v)(1). In addition, Defendants annually buy, receive, sell, or share for commercial purposes the Personal Information of more than 50,000 consumers.

174. Upon information and belief, Defendants violated Section 1798.150 of the CPPA by failing to prevent Plaintiffs and California Subclass Members' nonencrypted and nonredacted Personal Information from unauthorized access, and exfiltration, theft, or disclosure. These failures were the result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

175. As a direct and proximate result of Defendants' conduct, Plaintiffs' and the California Subclass Members' Personal Information, including names, dates of birth, Social Security numbers, and passcodes among other information, were subjected to unauthorized access, exfiltration, theft, or disclosure.

176. On information and belief, Plaintiffs allege that this Personal Information was not encrypted or redacted in the format accessed during the Data Breach.

177. Plaintiff and the California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereafter adequately safeguards customers' Personal Information by implementing reasonable enhanced security procedures and practices. Such relief is particularly important because Defendants continues to hold past and current customers' Personal Information, including that of Plaintiffs and California Subclass Members. These individuals have an interest in ensuring that their Personal Information is reasonably protected.

178. Simultaneously herewith, Plaintiffs are providing notice to Defendants pursuant to Cal. Civ. Code § 1798.150(b), identifying the specific provisions of the CCPA that Plaintiffs allege AT&T has violated or is violating.

179. Assuming Defendant cannot cure the Data Breach within 30 days—and Plaintiffs believe any such cure is not possible under these facts and circumstances—Plaintiffs will amend this complaint to pursue actual damages and statutory damages on behalf of the California Subclass Members as authorized by Cal. Civ. Code § 1798.150(a)(1)(A).

COUNT VII
Declaratory Judgment
(On behalf of Plaintiffs and the Nationwide Class against both Defendants)

180. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

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

182. An actual controversy has arisen in the wake of the Data Breach regarding AT&T's present and prospective common law and other duties to reasonably safeguard Personal Information and whether AT&T is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further cyberattacks and data breaches that could compromise their private Personal Information.

183. AT&T still possesses Personal Information pertaining to Plaintiffs and Class Members and continues to share this Personal Information with third parties, including its vendors, which means that Plaintiffs' and Class Members' Personal Information remains at risk of further breaches because AT&T's data security measures remain inadequate.

184. Plaintiffs and Class Members continue to suffer injuries as a result of the compromise of their Personal Information and remain at an imminent risk that subsequent compromises of their Personal Information will occur in the future.

185. Pursuant to the Declaratory Judgment Act, Plaintiffs and Class Members seek a declaration that: (a) AT&T's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) AT&T must have policies and procedures in place to ensure the parties with whom it shares sensitive Personal Information maintain reasonable, industry-standard security measures, including, but not limited to, those provided by the FTC or other governmental or regulatory industry guidelines, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class Members' Personal

Information if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging third-party security auditors or penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on AT&T's systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting Personal Information and segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner sensitive Personal Information not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and other industry-standard procedures to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and identify what to do in response to a breach.

VII. PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Classes as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are the proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendants from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiffs be granted the declaratory relief sought herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

///

///

///

VIII. JURY DEMAND

Plaintiffs hereby demand a trial by jury.

Dated: April 24, 2024

Respectfully submitted,

BERMAN TABACCO

By: */s/ Kristin J. Moody*
Kristin J. Moody

Pierce H. Stanley
425 California Street, Suite 2300
San Francisco, CA 94104
Telephone: (415) 433-3200
Email: kmoody@bermantabacco.com
pstanley@bermantabacco.com

Patrick T. Egan
BERMAN TABACCO
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
Email: pegan@bermantabacco.com

Counsel for Plaintiffs Mildred Kinchen and James Kinchen and the Proposed Classes