UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

TIMOTHY TRIMBLE, individually and on behalf of all others similarly situated, *Plaintiff*, v. AT&T MOBILITY LLC, *Defendant.*	**Civil Action No.:**_____ **CLASS ACTION COMPLAINT** **JURY TRIAL REQUESTED**

Plaintiff Timothy Trimble ("Plaintiff"), by and through counsel, on behalf of himself and others similarly situated brings this Class Action Complaint against AT&T Mobility LLC, ("Defendant" or "AT&T""). Upon personal knowledge, investigation of counsel, and upon information and belief, Plaintiff states and alleges as follows:

I. PRELIMINARY STATEMENT

1. Plaintiff seeks monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclass, as defined below. Plaintiff's personally-identifiable information ("PII") was exfiltrated and compromised in the data breach announced by AT&T on March 15, 2023 (the "Data Breach"), and Plaintiff brings this action on behalf of himself and all those similarly situated both across the United States and within his State of residence. Because only AT&T (and the cybercriminals who perpetrated the Data Breach) has knowledge of exactly what information was compromised, Plaintiff reserves his right to supplement these allegations with additional facts and injuries as they are discovered.

2. AT&T is one of the largest consumer brands in the United States. As of 2021, AT&T had a total of 201.79 million wireless subscribers[1] and collects immense amounts of personal identifying data related to its customers. Even with roughly 200 million paying customers, AT&T strives to increase its bottom line by selling this aforementioned personal identifying information.

3. AT&T understood it had an enormous responsibility to protect the data it collected and assured consumers through its Privacy Policy that AT&T believes "Your information and your privacy are important — to you and to us. This policy explains how we use your information and *how we keep it safe*." AT&T promises it's consumers that when AT&T gives third parties access to AT&T's customers' data, AT&T "do not allow those vendors to use your information for any purpose other than to perform those services, and *we require them to protect the confidentiality and security of data they get from us in a way that's consistent with this Policy*."[2]

4. AT&T completely and utterly failed to meet these obligations and protect sensitive consumer data. Even after experiencing large and consequential data breaches in April 2015, AT&T has once again suffered a massive data breach in and or around January 2023—which compromised the sensitive personal information of approximately 9 million consumers in the United States.

II. JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in

[1] https://www.statista.com/statistics/220692/number-of-atundt-wireless-subscribers-since-2007/ (Last visited 3/16/23)
[2] https://about.att.com/privacy/full_privacy_policy.html (Last visited 3/16/23)

controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendants are citizens of States different from that of at least one Class member.

6. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

7. This Court has personal jurisdiction over AT&T Mobility LLC, because it is authorized to and regularly conducts business in the State of North Carolina. AT&T sells, markets, and advertises its products and services to Plaintiff and Class Members located in the State of North Carolina and, therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

9. Defendant AT&T Mobility LLC is a Delaware limited liability company with its principal office or place of business at 1025 Lenox Park Boulevard NE, Atlanta, GA 30319. AT&T transacts business in this district and throughout the United States.

10. Plaintiff Timothy Trimble is a resident of the State of North Carolina and is a current customer of AT&T. Plaintiff has been an AT&T customer since 2013.

11. Plaintiff learned of the Data Breach via an email from AT&T sent soon after the Data Breach announcement in March 2023.

12. As a result of the Data Breach, Plaintiff spent significant time and effort in reviewing his various electronic accounts for fraudulent activity, the Data Breach, and a possible

remedy for the Data Breach. Plaintiff Trimble has noticed suspicious activity including elevated spam calls, texts, and emails.

13. Plaintiff places significant value in the security of his PII. Plaintiff entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

14. Given the sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm.

IV. FACTUAL ALLEGATIONS

A. AT&T Collects, Stores, and Profits from Consumer Information, and Promises to Keep it Secure.

15. AT&T is a U.S. wireless telecom and internet provider formed in 1876 following Alexander Graham Bell's development of the telephone. In 1984, the former AT&T agreed to divest its local telephone operations but retain its long distance, R&D, and manufacturing arms. From this, SBC Communications Inc. (first known as Southwestern Bell Corp.) was born. SBC expanded its U.S. presence through a series of acquisitions, including Pacific Telesis Group (1997) and Ameritech Corp. (1999). In 2005, SBC acquired AT&T Corp, creating the new AT&T, a leader in global communications for businesses. Following a series of mergers and acquisitions—including mergers with Cricket in 2013 and Lusacell and Nextel Mexico in 2015—AT&T grew to the one of the largest wireless carriers in the United States, with over 100 million current subscribers. AT&T is a publicly traded company organized and operated for the profit and financial benefit of its shareholders. In 2021, AT&T had annual gross revenues of over $134 billion, with net income over $19.87 billion.

16. AT&T has often attempted to distinguish itself from its competitors by promoting its purportedly unique customer experience. For example, on its website, AT&T states that: "As one of the largest advertisers in the U.S., AT&T strives to create marketing messages that accurately represent society as well as our products and services."[3]

17. To run its business, AT&T collects, maintains, and profits from the PII of millions of its U.S. consumers. PII is information that is used to confirm an individual's identity and can include an individual's name, Social Security number, driver's license number, phone number, financial information, and other identifying information unique to an individual. For AT&T, this information also includes unique technical identifiers tethered to customers' mobile phones. AT&T collects this PII from prospective and current customers and maintains and profits from the PII regardless of whether a potential customer eventually selects AT&T as a wireless carrier. AT&T also maintains the PII of former customers for an indefinite period of time.

18. Under the Customer Data Privacy section of their marketing page, AT&T states: "Data helps us create more reliable products and services, improve security and detect fraud, and provide customers with customized offers. Customers also count on AT&T to protect their information and respect their privacy. We take this responsibility seriously and work hard to maintain customers' trust."[4]

19. AT&T's Privacy Policy[5] states that it applies "information generated when you use or subscribe to AT&T products, services, apps, websites or networks to which this Policy is linked." Information, in this context, is about "you and how you're using our Products or Services along with information about your devices and equipment." This includes "data like

[3] https://about.att.com/csr/home/reporting/issue-brief/responsible-marketing.html (Last visited 3/16/23)
[4] *Id.*
[5] https://about.att.com/privacy/full_privacy_policy.html (Last visited 3/16/23)

your performance information, along with web browsing, location and video viewing information." It further states that the Notice applies to "anyone who uses our Products or Services under your account"[6]

20. The Privacy Policy provides customers with how AT&T uses customers' personal data to "provide, support, improve, protect, analyze and bill for our products, service and network; to communicate with consumer about consumer's service, products or apps; to better understand how consumers use our Products and Services; to market our services; to detect and avoid fraud; for advertising; and for research"; and to create "aggregate business and marketing insights, and help companies develop aggregate insights (for instance, to market or improve Products and Services). We aggregate the data before we share it, which means that we group the information so that it does not identify consumers personally, and we require anyone who receives this data to agree they will only use it for aggregate insights, won't attempt to identify any person or device using this information, and will handle it in a secure manner, consistent with this Policy."[7]

21. According to the Privacy Policy's California Privacy Rights section, included for purposes of complying with the California Consumer Protection Act ("CCPA"), AT&T states "We don't knowingly allow other parties to collect personally identifiable information about your online activities over time and across non-AT&T company websites for their own use when you use our websites and services, unless we have your consent."[8]

[6] *Id*.
[7] *Id*.
[8] *Id*.

22. AT&T essentially uses customer PII to "design[] and deliver[] advertising and marketing campaigns."[9]

23. AT&T agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: "with your consent or at your direction," "with the account holder," "between AT&T brands and companies," "to provide benefits," "to our service providers," "to other third parties for uses described in this notice or for purposes you have requested," "for identity verification and fraud prevention services," "caller ID providers," "in a business transfer or transaction" which is specified as a "corporate business transaction like an acquisition, divestiture, sale of company assets," and "for legal process and protection." None of the enumerated circumstances involve sharing Plaintiff's or the Class Members' PII with a criminal hacker.

24. After enumerating the ways it would limit the sharing of consumer's PII and also listing the ways AT&T benefits and profits from tracking and targeting its customers and noncustomers through collecting and maintaining their valuable PII, AT&T's Privacy Policy pledges to them that their PII is secure, stating that: (i) personal data will be disclosed only "with your consent, which we may get in writing, online, or orally," and (ii) AT&T uses "administrative, technical, contractual, and physical safeguards designed to protect your data." As discussed herein, AT&T failed to comply with these promises to protect Plaintiff's PII.

25. AT&T acknowledges that consumers "trust AT&T to connect you to the world every day, and we're working hard to earn a place in your heart. A big part of that is maintaining your privacy. We believe you deserve transparency, education, choice, protection, and

[9] *Id*.

simplicity." These assurances have proved hollow for the millions of consumers affected by AT&T's breach of trust and failure to protect their PII.

B. Despite Its Promises, AT&T Failed to Protective Sensitive PII

26. At the same time AT&T collected, stored, and profited from Plaintiff's PII—and was actively communicating to consumers that they can "trust" AT&T with their sensitive data—it suffered a massive data breach compromising the PII of millions of its customers.

27. On March 15, 2023, AT&T announced that a "bad actor" had compromised the PII of "approximately 9 million customer accounts."[10]

28. This Data Breach occurred sometime in January 2023.[11]

29. Although AT&T has released very little information about the Data Breach, it has stated that its customers PII was compromised through a "Customer Proprietary Network Information" or "CPNI."[12]

30. CPNI in the United States is information that telecommunications services (such as local, long-distance and wireless telephone companies) acquire from their subscribers. It includes what services subscribers use, as well as the type of usage and usage amount.[13]

31. Upon detection, AT&T stated that it "promptly notified law enforcement," and "information such as first names, wireless account numbers, wireless phone numbers and even email addresses was included in the breach."[14]

---

[10] https://www.ksstradio.com/2023/03/9-million-att-customers-affected-in-data-breach/ (Last visited 3/16/23)
[11] https://www.foxnews.com/tech/att-reveals-data-breach-affecting-9-million-wireless-accounts
[12] *Id.*
[13] https://www.techtarget.com/searchnetworking/definition/CPNI (Last visited 3/16/23)
[14] https://www.ksstradio.com/2023/03/9-million-att-customers-affected-in-data-breach/ (Last visited 3/17/23)

32. The categories of PII compromised in the Data Breach include but are not limited to "name, billing address, email, phone number, date of birth, account number, and information such as the number of lines on the account and service plan features."[15]

C. AT&T Compounded Its Failure By Providing Inadequate Notice.

33. AT&T has stated that it has "notified certain federal agencies about the incident" and has "begun notifying customers whose information may have been obtained by the bad actor in accordance with applicable state and federal requirements."[16]

34. However, notices sent to and received by victims of the Data Breach are woefully deficient. Instead of warning Data Breach victims that they are at significant risk of identity theft and fraud, the AT&T notice states AT&T "prevented the most sensitive types of customer information from being accessed," and that "[c]ustomer accounts and finances [were] not put directly at risk by this event."[17]

35. Likewise, in its press release, AT&T tried to downplay the value of what was stolen stating that it believed "The exposed data didn't include Social Security numbers, credit card information, account passwords or 'other sensitive information'" and asserting that "mostly related to device upgrade eligibility."[18]

36. However, this is misleading as the PII compromised in the Data Breach significantly increases the risk of identity theft and fraud for victims. For example, Chester Wisniewski, field chief technical officer of applied research at the security firm Sophos, stated that "[t]he information stolen in this breach is ideal for SIM swapping attacks and other forms of

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] https://www.cnet.com/tech/mobile/at-t-vendor-data-breach-exposed-9-million-customer-accounts/

identity theft," which "should be another reason for AT&T customers to lock down their accounts" for financial accounts.

37. Similarly, Justin Fier, a senior vice president for the security company Darktrace, stated that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates: "There are dozens of ways that the information that was stolen could be weaponized."

38. AT&T's efforts to notify Plaintiff and Class Members thus fell short of providing key information about the Data Breach, consisting of brief messages with little substantive information that failed to warn victims to take action to protect themselves from identity theft and fraud.

39. AT&T's deficient notices compounded the harm suffered by Plaintiff and Class Members, by failing to timely provide Breach victims with the very details necessary to protect themselves.

D. AT&T Has History Of Significant Data Breaches.

40. The Breach and resulting harm suffered by Plaintiff and Class Members is directly attributable to AT&T's security lapses and data mismanagement. Indeed, AT&T is no stranger to cybersecurity incidents resulting from its flawed security. Rather, multiple data breaches have occurred in the past decade.

41. In 2015, AT&T agreed, in cooperation with the Federal Communications Commission to pay $25 Million to settle three consumer privacy investigations.[19]

42. In May 2014, the Enforcement Bureau launched its investigation into a 168-day data breach that took place at an AT&T call center in Mexico between November 2013 and April

[19] https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0

2014. During this period, three call center employees were paid by third parties to obtain customer information — specifically, names and at least the last four digits of customers' Social Security numbers — that could then be used to submit online requests for cellular handset unlock codes. The three call center employees accessed more than 68,000 accounts without customer authorization, which they then provided to third parties who used that information to submit 290,803 handset unlock requests through AT&T's online customer unlock request portal.

43. According to a subsequent investigation by the FCC's Enforcement Bureau, these data breaches occurred when employees at call centers used by AT&T in Mexico, Colombia, and the Philippines accessed customer records without authorization. These employees accessed CPNI while obtaining other personal information that was used to request handset unlock codes for AT&T mobile phones, and then provided that information to unauthorized third parties who appear to have been trafficking in stolen cell phones or secondary market phones that they wanted to unlock.[20]

44. At that time, FCC Chairman Tom Wheeler stated: "As the nation's expert agency on communications networks, the Commission cannot — and will not — stand idly by when a carrier's lax data security practices expose the personal information of hundreds of thousands of the most vulnerable Americans to identity theft and fraud."[21]

45. Given the numerous data breaches pre-dating the Breach at issue in this case, AT&T was clearly aware of its data security failures, and the fact that subsequent breaches have occurred reinforces that Plaintiff's PII, which remains in AT&T's possession, is not safe.

[20] *Id.*
[21] *Id.*

E. AT&T Failed To Comply With Regulatory Guidance And Industry-Standard Cybersecurity Practices.

46. AT&T's well-documented history of data security failure is attributable to its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII.

47. For example, at least 24 states have enacted laws addressing data security practice that require that businesses that own, license or maintain PII to implement and maintain reasonable security procedures and practices and to protect PII from unauthorized access. North Carolina is one of these states. North Carolina requires a business to provide adequate notice of a security breach to its customers. See N.C. Gen. Stat. § 75-60. Also, North Carolina requires certain businesses, in regard to cybersecurity: "Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system." See N.C. Gen. Stat. § 75-65.

48. AT&T also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

49. The FTC recommends:

i. limiting access to customer information to employees who have a business reason to see it;

ii. keeping customer information in encrypted files provides better protection in case of theft;

iii. maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;

iv. using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;

v. monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,

vi. monitoring activity logs for signs of unauthorized access to customer information.[22]

50. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

51. In 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established guidelines for fundamental data security principles and practices for

[22] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

[23] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

business.[24] The guidelines note businesses should protect the personal customer information they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

52. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

54. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

55. 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

[24] Federal Trade Commission, Protecting PII: A Guide for Business, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

57. AT&T was aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers' PII from unauthorized access.

58. In this case, AT&T was at all times fully aware of its obligation to protect the PII of its customers. AT&T was also aware of the significant repercussions if it failed to do so because AT&T collected PII from millions of consumers and it knew that this PII hacked, would result in injury to consumers, including Plaintiff and Class Members.

59. Based upon the known details of the Data Breach and how it occurred, AT&T also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and prevention.

F. The Effect Of The Data Breach On Plaintiff and Class Members.

60. AT&T's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach, hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future.

61. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

62. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

63. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."

64. There is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor his accounts for years to ensure his PII obtained in the Data Breach is not used to harm him. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach. In other words, Plaintiff has been harmed by the value of identity protection services he must purchase in the future to ameliorate the risk of harm he now faces due to the Breach.

65. Plaintiff and Class Members have also realized harm in the lost or reduced value of their PII. AT&T admits the PII compromised in the Breach is valuable. As discussed above, AT&T collects, retains, and uses Plaintiff's PII to increase profits through predictive and other targeted marketing campaigns. Plaintiff's PII is not only valuable to AT&T, but Plaintiff also

places value on his PII based on his understanding that his PII is a financial asset to companies that collect it.[25]

66. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiff's PII that was permitted without authorization by AT&T. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

67. Plaintiff and Class Members value the privacy of this information and expect AT&T to allocate enough resources to ensure it is adequately protected. Customers would not have done business with AT&T, provided their PII and payment card information, or paid the same prices for AT&T's goods and services had they known AT&T did not implement reasonable security measures to protect their PII Customers reasonably expect that the payments they make to the carrier, either prepaid or each month, incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiff and Class Members did not receive the benefit of their bargain with AT&T because they paid a value for services they expected but did not receive.

68. Given AT&T's failure to protect Plaintiff's and the Class Members' PII despite multiple data breaches in the past as well as subsequent data breaches, Plaintiff has a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary

[25] *See*, e.g., *Ponemon Institute, LLC, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70), available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

damages, restitution, or disgorgement) that protects him from suffering further harm, as his PII remains in AT&T's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

69. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the lost value of access to Plaintiff's and Class Members' PII permitted by AT&T; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; (vi) AT&T's retention of profits attributable to Plaintiff's and Class Members' PII that AT&T failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to AT&T for goods and services purchased, as Plaintiff reasonably believed a portion of the sale price would fund reasonable security measures that would protect his PII, which was not the case; and (x) nominal damages.

V. CLASS ALLEGATIONS

a. NATIONWIDE CLASS

70. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following Nationwide Class (the "Nationwide Class" or the "Class"):

"*All natural persons residing in the United States whose PII was exfiltrated in the AT&T Data Breach that occurred in and or around January 2023*."

71. The Nationwide Class asserts claims against AT&T for negligence (Count 1), negligence per se (Count 2), breach of confidence (Count 3), intrusion upon seclusion (Count 4), breach of express contract (Count 5), breach of implied contract (Count 6), unjust enrichment (Count 7), and declaratory judgment (Count 8).

b. North Carolina Subclass

72. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of a North Carolina Subclass in the alternative to the nationwide claims (Counts 1 through 8), as well as with respect to statutory claims under N.C. Gen. Stat. § 75-65 (Count 9), on behalf of a North Carolina Subclass, defined as follows:

"*All natural persons residing in North Carolina whose PII was exfiltrated in the AT&T Data Breach that occurred in and or around January 2023*."

73. Excluded from the Nationwide Class and the North Carolina Subclass (collectively, the "Class") are AT&T, any entity in which AT&T has a controlling interest, and AT&T's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff.

74. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of the Nationwide Class and the North Carolina Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, AT&T has acknowledged that millions of individuals' PII has been compromised. Those individuals' names and addresses are available from AT&T's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are

at least thousands of individuals in the Nationwide Class and at least thousands of individuals in the North Carolina Statewide Subclass, making joinder of all Class Members impracticable.

75. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3)**. As to both the Nationwide Class and the North Carolina Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include, but are not limited to,:

a. Whether AT&T had a duty to protect PII;

b. Whether AT&T failed to take reasonable and prudent security measures to ensure its systems were protected;

c. Whether AT&T failed to take available steps to prevent and stop the Breach from happening;

d. Whether AT&T knew or should have known that its computer and data storage systems were vulnerable to attack;

e. Whether AT&T was negligent in failing to implement reasonable and adequate security procedures and practices;

f. Whether AT&T's security measures to protect its systems were reasonable in light known legal requirements;

g. Whether AT&T's conduct constituted unfair or deceptive trade practices';

h. Whether AT&T violated state or federal law when it failed to implement reasonable security procedures and practices;

i. Which security procedures and notification procedures AT&T should be required to implement;

j. Whether AT&T has a contractual obligation to provide for the security of customer PII;

k. Whether AT&T has complied with any contractual obligations to protect customer PII;

l. What security measures, if any, must be implemented by AT&T to comply with its contractual obligations;

m. Whether AT&T violated state consumer protection laws in connection with the actions described herein;

n. Whether AT&T failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Data Breach was discovered;

o. Whether AT&T conduct resulted in or was the proximate cause of the loss of the PII of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of AT&T's failure to reasonably protect their PII;

q. Whether AT&T should retain the money paid by Plaintiff and Class Members to protect their PII, and the profits AT&T generated using Plaintiff's and Class Members' PII;

r. Whether AT&T should retain Plaintiff's and Class Members' valuable PII; and,

s. Whether Plaintiff and Class Members are entitled to damages or injunctive relief.

76. **Typicality: Federal Rule of Civil Procedure 23(a)(3)**. As to the Nationwide Class and the North Carolina Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's PII was in AT&T's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and

injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

77. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4)**. Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Nationwide Class and the North Carolina Subclass because Plaintiff is a member of the Nationwide Class and the North Carolina Subclass and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

78. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3)**. Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against AT&T, and thus, individual litigation to redress AT&T's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and

the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

79. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for AT&T or would be dispositive of the interests of members of the proposed Class.

80. **Ascertainability**. The Nationwide Class and North Carolina Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Nationwide Class and North Carolina Subclass consist of individuals who provided their PII to AT&T. Class Membership can be determined using AT&T's records.

81. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

82. 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.

COUNT ONE: NEGLIGENCE
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

83. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

84. AT&T required Plaintiff and Class Members to submit sensitive PII in order to obtain or apply for its products and services.

85. AT&T owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons.

86. More specifically, this duty included, among other things: (a) designing, maintaining, and testing AT&T's security systems to ensure that Plaintiff's and Class Members' PII in AT&T's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

87. AT&T's duty to use reasonable care arose from several sources, including but not limited to those described herein.

88. AT&T had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by AT&T's failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, AT&T knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

89. AT&T's duty to use reasonable security measures also arose as a result of the special relationship that existed between AT&T, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted AT&T with their PII as part of the applications for or purchase and signing-up for the products and services AT&T offers as a major telecommunications company. AT&T alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

90. AT&T's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as AT&T. Various FTC publications and data security breach orders further form the basis of AT&T's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

91. AT&T's duty also arose from AT&T's unique position as one of the largest wireless carrier in the United States. As a telecommunications company, AT&T holds itself as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiff and Class Members. AT&T has stated to consumers that: "Your information and your privacy are important — to you and to us. This policy explains how we use your information and how we keep it safe."[26] Because of its role as the second largest wireless carrier, AT&T was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the AT&T Data Breach.

[26] https://about.att.com/privacy/full_privacy_policy.html

92. AT&T admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

93. With regard to network security, AT&T further acknowledges that it "use[s] administrative, technical, contractual, and physical safeguards designed to protect your data."[27]

94. AT&T knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

95. AT&T also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require AT&T to reasonably safeguard sensitive PII, as detailed herein.

96. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by AT&T's misconduct.

97. Instead of issuing notice within a reasonable time of the breach that occurred in or around January of 2023, AT&T waited until March 8, 2023 to notify Plaintiff and Class Members for the January Data Breach.

[27] *Id*.

98. AT&T breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. AT&T breached these duties by, among other things, failing to:

a. exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members;

b. detect the Breach while it was ongoing;

c. maintain security systems consistent with industry standards during the period of the Data Breach;

d. comply with regulations protecting the PII at issue during the period of the Data Breach; and

e. disclose in a timely and adequate manner that Plaintiff's and the Class Members' PII in AT&T's possession had been or was reasonably believed to have been, stolen or compromised.

99. But for AT&T's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

100. AT&T's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

101. Plaintiff and Class Members were foreseeable victims of AT&T's inadequate data security practices, and it was also foreseeable that AT&T's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

102. As a direct and proximate result of AT&T's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such

injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and noneconomic harm.

COUNT TWO: NEGLIGENCE PER SE
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALFOF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

103. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

104. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as AT&T of failing to use reasonable measures to protect PII.

105. The FTC publication and orders also form the basis of AT&T's duty.

106. AT&T violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. AT&T's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as AT&T, including, specifically the damages that would result to Plaintiff and Class Members.

107. In addition, under state data security statutes, AT&T had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII.

108. AT&T's failure to safeguard Plaintiff's and Class Members' PII is a violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

109. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

110. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

111. AT&T breached its duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

112. Plaintiff and Class Members were foreseeable victims of AT&T's violations of the FTC Act and state data security statutes. AT&T knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

113. But for AT&T's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII would not have been accessed by unauthorized parties.

114. As a direct and proximate result of AT&T's negligence per se, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and noneconomic harm.

COUNT THREE: BREACH OF CONFIDENCE (ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALFOF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

115. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

116. Plaintiff and Class Members maintained a confidential relationship with AT&T whereby AT&T undertook a duty not to disclose to unauthorized parties the PII provided by

Plaintiff and Class Members to AT&T to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

117. AT&T knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

118. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because AT&T failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

119. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

120. But for AT&T's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. AT&T's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

121. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of AT&T's unauthorized disclosure of Plaintiff's and Class Members' PII. AT&T knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' PII had serious security vulnerabilities because AT&T failed to observe even basic information security practices or correct known security vulnerabilities.

122. As a direct and proximate result of AT&T's breach of confidence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT FOUR: INVASION OF PRIVACY
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

123. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

124. Plaintiff shared PII with AT&T that Plaintiff wanted to remain private and nonpublic.

125. Plaintiff reasonably expected that the PII Plaintiff shared with AT&T would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

126. AT&T intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

127. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, AT&T unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

128. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

129. AT&T's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

130. As a direct and proximate result of AT&T's invasions of privacy, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic

harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and noneconomic harm.

COUNT FIVE: BREACH OF EXPRESS CONTRACT
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

131. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

132. AT&T's Privacy Notice is an agreement between AT&T and individuals who provided their PII to AT&T, including Plaintiff and Class Members.

133. AT&T's Privacy Notice states that it applies "the information generated when you use or subscribe to AT&T products, services, apps, websites or networks to which this Policy is linked.," meaning "data that identifies, relates to, describes, can be associated with, or could reasonably identify you as an individual and consumer." This includes "Account Information, Web browsing and app information, equipment information, network performance and usage information, location information, and biometric information."

134. AT&T's Privacy Notice stated at the time of the Data Breach that AT&T "use[s] administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control."[28]

135. AT&T further agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: "with your consent or at your direction," "with the account holder," "between AT&T brands and companies," "to provide benefits," "to our service providers," "to other third parties . . . for uses described in this notice or for purposes you have requested," "for identity verification and fraud prevention services," "caller ID providers," "in a business transfer or transaction" which is specified as a "corporate business transaction like an acquisition, divestiture, sale of company assets," and "for legal process and protection."[29] None of the enumerated circumstances involve sharing Plaintiff's or the Class Members' PII with a criminal hacker.

136. AT&T's emphasized in its Privacy Policy at the time of the Data Breach that those who provide their PII to AT&T "Your information and your privacy are important — to you and to us."[30] Plaintiff and Class Members on the one side and AT&T on the other formed a contract when Plaintiff and Class Members obtained products or services from AT&T, or otherwise provided PII to AT&T subject to its Privacy Policy.

137. Plaintiff and Class Members fully performed their obligations under the contracts with AT&T.

138. AT&T breached its agreement with Plaintiff and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems

[28] https://about.att.com/privacy/full_privacy_policy.html
[29] *Id*.
[30] *Id*.

to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

139. As a direct and proximate result of AT&T's breach of contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

140. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT SIX: BREACH OF IMPLIED CONTRACT (ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

141. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

142. Plaintiff and Class Members entered into an implied contract with AT&T when they obtained products or services from AT&T, or otherwise provided PII to AT&T.

143. As part of these transactions, AT&T agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII was breached or compromised.

144. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that AT&T's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiff and Class Members believed that AT&T would use part of the monies paid to AT&T under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security practices.

145. Plaintiff and Class Members would not have provided and entrusted their PII to AT&T or would have paid less for AT&T products or services in the absence of the implied contract or implied terms between them and AT&T. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

146. Plaintiff and Class Members fully performed their obligations under the implied contracts with AT&T.

147. AT&T breached its implied contracts with Plaintiff and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

148. As a direct and proximate result of AT&T's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and

economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT SEVEN: UNJUST ENRICHMENT
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALFOF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

149. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

150. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by AT&T and that was ultimately stolen in the AT&T Data Breach.

151. AT&T was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information. AT&T understood that it was in fact so benefitted.

152. AT&T also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon AT&T maintaining the privacy and confidentiality of that PII.

153. But for AT&T's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with AT&T.

154. AT&T admits that it uses the PII it collects for, among other things, advertising and marketing "products and services from AT&T and other companies to you, including through targeted advertising and communications about promotions and events, contents, and sweepstakes," and conducting research and creating reports "from analysis of things like usage patterns and trends and to deidentify or aggregate personal data to create business and market analysis and reports."[31]

155. Because of its use of Plaintiff's and Class Members' PII, AT&T sold more services and products than it otherwise would have. AT&T was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

156. AT&T also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

157. AT&T also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiff's and Class Members' PII.

158. It is inequitable for AT&T to retain these benefits.

159. As a result of AT&T's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data

[31] *Id.*

security measures, and its other conduct facilitating the theft of that PII), AT&T has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

160. AT&T's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

161. It is inequitable, unfair, and unjust for AT&T to retain these wrongfully obtained benefits. AT&T's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

162. The benefit conferred upon, received, and enjoyed by AT&T was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for AT&T to retain the benefit.

163. AT&T's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class Members other damages as described herein.

164. Plaintiff and the Class Members have no adequate remedy at law.

165. AT&T is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on AT&T as a result of its wrongful conduct, including specifically: the value to AT&T of the PII that was stolen in the Data Breach; the profits AT&T received and is receiving from the use of that information; the amounts that AT&T overcharged Plaintiff and Class Members for use of AT&T's products and services; and

the amounts that AT&T should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

COUNT EIGHT: VIOLATION 28 U.S.C. §§2201 et seq.,
DECLARATORY JUDGEMENT
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

166. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

167. 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. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

168. An actual controversy has arisen in the wake of the AT&T Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether AT&T is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff continues to suffer injury as a result of the compromise of Plaintiff's PII and remain at imminent risk that further compromises of his PII will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII stored by AT&T.

169. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AT&T continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. AT&T continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

170. The Court also should issue corresponding prospective injunctive relief requiring AT&T to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

171. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at AT&T. The risk of another such breach is real, immediate, and substantial. If another breach at AT&T occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

172. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to AT&T if an injunction is issued. Among other things, if another massive data breach occurs at AT&T, Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to AT&T of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and AT&T has a pre-existing legal obligation to employ such measures.

173. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AT&T, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

COUNT NINE: VIOLATION OF N.C. Gen. Stat. § 75-60
"IDENTITY THEFT PROTECTION ACT"
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE NORTH CAROLINA SUBCLASS)

174. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

175. In pertinent part, N.C. Gen. Stat. § 75-65 provides:

> Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

176. N.C. Gen. Stat. § 14-113.20b defines "Personal Information" as a person's first name or initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State:

a. Social security or employer taxpayer identification numbers;[32]

b. Drivers license, State identification card, or passport numbers;[33]

c. Financial account number, or credit card or debit card number; [34]

d. Personal Identification Code, electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names, digital signatures[35] ;

e. "any other numbers or information that can be used to access a person's financial resources" [36] ;

[32] North Carolina General Statute § 14-113.20(b)(1)
[33] North Carolina General Statute § 14-113.20(b)(2)
[34] North Carolina General Statute § 14-113.20(b)(3)-(6)
[35] North Carolina General Statute § 14-113.20(b)(7)-(9)

f. biometric data, fingerprints, passwords, legal surname prior to marriage.[37]

177. Defendant owns, licenses and/or maintains computerized data that includes Plaintiff's and Class Members' PII.

178. Defendant's conduct, as alleged above, violated the Identity Theft Protection Act of North Carolina, N.C. Gen. Stat. § 75-60.

179. Defendant was required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber security incident described herein.

180. AT&T's Data Breach constituted a "Security breach" 7 within the meaning of N.C. Gen. Stat. § 75-60.

181. The information compromised in AT&T's Data Breach constituted "personal identifying information" within the meaning of N.C. Gen. Stat. § 75-60.

182. Defendant violated N.C. Gen. Stat. § 75-60 by unreasonably delaying disclosure of the Data Breach to Plaintiff and Class Members, whose personal identifying information was, or reasonably believed to have been, acquired by an unauthorized person.

183. As a result of Defendant's violation of N.C. Gen. Stat. § 75-60, Plaintiff and Class

184. Members incurred damages as alleged herein.

185. Plaintiff, individually and on behalf of the Class, seeks all remedies available under N.C. Gen. Stat. § 75-60, including, but not limited to:

a. actual damages suffered by Class Members as alleged above;

b. statutory damages for Defendant's willful, intentional, and/or reckless conduct;

c. equitable relief; and

---

[36] North Carolina General Statute § 14-113.20(b)(10)
[37] North Carolina General Statute § 14-113.20(b)(11)-(14)

d. reasonable attorneys' fees and costs.

VI. REQUEST FOR RELIEF

186. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

187. Plaintiff, individually and on behalf of members of the Nationwide Class and North Carolina Subclass, as applicable, respectfully requests that the Court enter judgment in Plaintiff's favor and against AT&T, as follows:

188. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

189. That the Court grant permanent injunctive relief to prohibit AT&T from continuing to engage in the unlawful acts, omissions, and practices described herein, including;

a. Prohibiting AT&T from engaging in the wrongful and unlawful acts described herein;

b. Requiring AT&T to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring AT&T to delete, destroy, and purge the PII of Plaintiff and Class Members unless AT&T can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. Requiring AT&T to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. Requiring AT&T to engage independent third-party security auditors/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 AT&T to promptly correct any problems or issues detected by such third-party security auditors; Requiring AT&T to engage independent third-party security auditors and internal personnel to run automated security monitoring;

f. Requiring AT&T to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring AT&T to audit, test, and train its security personnel regarding any new or modified procedures; Requiring AT&T to segment data by, among other things, creating firewalls and access controls so that if one area of AT&T's network is compromised, hackers cannot gain access to other portions of AT&T's systems;

h. Requiring AT&T to conduct regular database scanning and securing checks;

i. Requiring AT&T to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. Requiring AT&T to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

k. Requiring AT&T to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with AT&T's policies, programs and systems for protecting PII; Requiring AT&T to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor AT&T's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l. Requiring AT&T to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor AT&T's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

m. Requiring AT&T to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

n. Requiring AT&T to implement logging and monitoring programs sufficient to track traffic to and from AT&T servers; and

o. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis AT&T's compliance with the terms of the Court's final judgment, to provide such

report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

190. That the Court award Plaintiff and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

191. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by AT&T as a result of its unlawful acts, omissions, and practices;

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

193. That Plaintiff be granted the declaratory relief sought herein;

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

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

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

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff hereby demands a trial by jury on all issues so triable.

[signature on following page]

Dated: March 16, 2023

/s/Blake G. Abbott
Blake G. Abbott (N.C. Bar No. 57190)
Paul Doolittle (*Pro Hac Vice Forthcoming*)
Poulin | Willey | Anastopoulo, LLC
32 Ann Street
Charleston, SC 29403
803-222-2222
Email: blake@akimlawfirm.com
pauld@akimlawfirm.com

UNITED STATES DISTRICT COURT
for the
Western District of North Carolina

TIMOTHY TRIMBLE,individually and on behalf of all others similarly situated,

Plaintiff)
v.) **Civil Action No.**
)
AT&T Mobility, LLC)
)
)
)
)
Defendant

SUMMONS IN A CIVIL ACTION

TO: ***(Defendant's name and address)***

AT&T Mobility, LLC
1025 Lenox Park Boulevard NE
Atlanta, GA 30319

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) – or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12(a)(2) or (3) – you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Blake G. Abbott
Paul J. Doolittle
Poulin | Willey | Anastopoulo, LLC
32 Ann Street
Charleston, SC 29403

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4(1))

This summon for *(name of individual and title, if any)*
_____
was received by me on *(date)* _____.

❑ **I personally served the summons on the defendant at *(place)*_____ on *(date)* _____; or**

❑ **I left the summons at the individual's residence or usual place of abode with *(name)* _____, a person of suitable age and discretion who resides there, on *(date)* _____, and mailed a copy to the individual's last known address; or**

❑ **I served the summons on *(name of individual)* _____, who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____; or**

❑ **I returned the summons unexecuted because _____; or**

❑ **Other *(specify)*:**
_____

My fees are $ _____ for travel and $ _____ for services, for a total of $_____.

I declare under penalty of perjury that this information is true.

Date:_____ **_____**
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Timothy Trimble

(b) County of Residence of First Listed Plaintiff Wilkes
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Poulin | Willey | Anastopoulo, LLC
32 Ann Street, Charleston, SC 29403 ; 803-222-2222

DEFENDANTS

AT&T Mobility, LLC

County of Residence of First Listed Defendant DeKalb, GA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332 ; Pub. L. No. 109-2, Class Action Fairness Act of 2005 ("CAFA")

Brief description of cause:
Class action suit stemming from online data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ $5,000,000+

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Mar 16, 2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Blake G. Abbott

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.