UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

TERRI LYNN HODGE, individually and on behalf of all similarly situated, Plaintiff, v. AT&T MOBILITY LLC and AT&T, INC., Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Terri Lynn Hodge, by and through the undersigned counsel, brings this class action against Defendant AT&T Mobility LLC and Defendant AT&T, Inc. (collectively, "AT&T" or "Defendants"), on behalf of herself and all others similarly situated. Plaintiff makes the following allegations based on personal knowledge as to her own actions and on information and belief as to all other matters.

NATURE OF THE ACTION

1. In 2021, AT&T learned of a purported online auction of a database containing sensitive personal information belonging to 73 million of its customers—including their names, dates of birth, Social Security numbers, and other information. When questioned by reporters, AT&T denied any such information was taken from its systems and declined to comment on whether its third-party vendors

could have been involved. AT&T ignored the possibility of this enormous data breach and continued with its usual operations.

2. By March 2024, however, this data was made freely available on the dark web, causing AT&T to acknowledge at last that sensitive information belonging to tens of millions of its customers, past and present, had indeed been breached (the "Data Breach"). This included information AT&T required its customers to hand over to purchase its services, including their full name, email address, mailing address, phone number, Social Security number, date of birth, and AT&T account number and passcode (collectively, "PII").

3. To date, AT&T apparently cannot identify how, when, or where the breach occurred, despite being the largest mobile telecommunications provider in the United States. Upon first learning of the likely existence of this breach three years prior, the company did not investigate any details—until its recent publication on the dark web. Had AT&T done so and informed its customers of the Data Breach, they could have taken steps to protect themselves, their finances, and their financial reputations from further preventable harm.

4. The Data Breach, and the harm it caused and will cause AT&T's customers, are a result of AT&T's failures to adopt reasonable procedures and practices for information security, to exercise appropriate managerial control over

its third-party partners' information security, and to notify the Data Breach victims in a timely manner.

5. Plaintiff and Class members must now live with a significant risk of financial fraud, identity theft, identity-related fraud and other harms indefinitely, for which they seek to recover in this action for damages and other relief.

PARTIES

6. Plaintiff Terri Lynn Hodge is a citizen and resident of Texas whose PII was compromised from AT&T.

7. Defendant AT&T Mobility LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia. Defendant AT&T Mobility is a wholly owned subsidiary of Defendant AT&T, Inc.

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

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and some members of the proposed Class have a different citizenship from Defendants. This Court has supplemental jurisdiction over the state law claims

pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

10. This Court has jurisdiction over Defendant AT&T Mobility LLC because Defendant AT&T Mobility LLC maintains and operates its headquarters in this District. Defendant is authorized to conduct business in this District and is subject to general personal jurisdiction in this state.

11. This Court has jurisdiction over Defendant AT&T Inc. because AT&T has committed acts within the Northern District of Georgia giving rise to this action and has established minimum contacts within this forum such that the exercise of jurisdiction over AT&T Inc. would not offend traditional notions of fair play and substantial justice. AT&T has engaged in continuous, systematic, and substantial activities within this State, including substantial marketing and sales of services and products in connection with the Data Breach within this State.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to this action occurred in this District, including unknown actors' accessing, copying, and exfiltrating the PII of AT&T's customers.

FACTUAL ALLEGATIONS

AT&T's Privacy Practices

13. AT&T is the largest provider of telephone services, including mobile telephone services, in the United States, where it services hundreds of millions of wireless customers. In providing these services, it requires its wireless customers to provide personal information such as their names, addresses, dates of birth, and Social Security numbers. Contracting customers' highly sensitive PII is thereafter housed on AT&T's servers.

14. AT&T maintains privacy policies that explain how it handles customers' personal information. AT&T represents to its customers and potential customers that it employs robust security features to secure customer PII. AT&T also represents that it has a responsibility and commitment to protecting that PII—that it "work[s] hard to safeguard [customers'] information using technology controls and organizational controls";[1] "limit[s] access to personal information to the people who need access for their jobs";[2] and will "destroy [the PII] by making it unreadable or indecipherable"[3] once no longer needed for "business, tax or legal purposes." AT&T also states that it will "notify [customers] as required by law" if that data is

[1] *AT&T Privacy Notice*, AT&T, https://about.att.com/privacy/privacy-notice.html (last visited Apr. 4, 2024).
[2] *Id.*
[3] *Id.*

breached.[4] As a major firm handling sensitive PII, AT&T understood the importance of protecting customers' PII through data security.

AT&T Customers' PII Leaks on the Dark Web

15. AT&T learned of the Data Breach years ago. In August 2021, a group of hackers named ShinyHunters offered to sell "AT&T Database 70+M (SSN/DOB)" on a forum and marketplace for hackers.[5] ShinyHunters listed a starting bid of $200,000, or an immediate sale price of $1 million.

16. AT&T claimed that this data did not appear to come from its own servers.[6] When the company was pressed on whether the data could have been stolen from one of its partners, it stated that it could not "speculate on where it came from or whether it is valid."[7]

17. In March 2024, a person going by the name of MajorNelson leaked the ShinyHunters database for free on a hacking forum.[8] The leak included names, addresses, birthdates, mobile numbers, and Social Security numbers.

---

[4] *Id.*
[5] Waqas, *AT&T breach? ShinyHunters selling AT&T database with 70 million SSN*, HACKREAD (Aug. 20, 2021), https://www.hackread.com/att-breach=shinyhunters-database-selling-70-million-ssn/.
[6] Lawrence Abrams, *AT&T denies data breach after hacker auctions 70 milliion user database*, BLEEPING COMPUTER (Aug. 20, 2021, 9:43 a.m.).
[7] *Id.*
[8] Lawrence Abrams, *AT&T says leaked data of 70 million people is not from its systems,* BLEEPINGCOMPUTER (Mar. 17, 2024, 7:24 PM),

18. AT&T has issued a statement confirming the legitimacy of the leaked data:

> AT&T has determined that AT&T data-specific fields were contained in the data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set, which includes personal information such as social security numbers, the source of the data is still being assessed.
>
> AT&T has launched a robust investigation supported by internal and external cybersecurity experts. Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.
>
> Currently, AT&T does not have evidence of unauthorized access to its systems resulting in exfiltration of the data set. The company is communicating proactively with those impacted and will be offering credit monitoring at our expense where applicable. We encourage current and former customers with questions to visit www.att.com/accountsafety for more information.
>
> As of today, this incident has not had a material impact on AT&T's operations.

19. The Data Breach has been linked to the August 2021 auction of the data by ShinyHunters. One cybersecurity expert in consumer data said the data "closely resembles a similar data breach that surfaced in 2021 . . . ."[9] This expert verified the

---

https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70- million-people-is-not-from-its-systems/.

[9] https://apnews.com/article/att-data-breach-dark-web-passcodes-fbef4afe0c1deec9ffb470f2ec134f41

posted information through his network of nearly 5 million subscribers, which confirmed that over 150,000 of them were included in the data set.[10] This expert also contacted some potential victims directly, who confirmed it was in fact their data.

20. In the three years between the online auction listing and the posting of the breached data, AT&T did not launch an investigation or take any steps indicating it took the theft of its customers' data serious. The company still has not determined whether its systems or those of a third-party partner were breached to obtain the data.

AT&T Could Have Foreseen and Prevented the Data Breach

21. Despite claiming after the Data Breach that it takes "cybersecurity very seriously" and has a "fundamental commitment" to privacy, AT&T did not have strong protections in place to detect and stop this breach. It also did not exercise sufficient control or management of its third-party partners' data despite knowing they too stored its customers' PII and are prime targets for cyberattacks, which can impose significant costs on customers.

22. In 2022, the Federal Bureau of Investigation, National Security Agency, and the Cybersecurity and Infrastructure Security Agency (CISA) wrote a Cybersecurity Advisory warning of "[t]elecommunications and network service provider targeting."[11] The Advisory explained how cyber actors access network

[10] https://www.troyhunt.com/inside-the-massive-alleged-att-data-breach/
[11] *People's Republic of China State-Sponsored Cyber Actors Exploit*

service providers and other telecommunications organizations through open-source tools allowing for the scanning of IP addresses for vulnerabilities. After gaining an initial foothold, these actors identify "critical users and infrastructure including systems critical to maintaining the security of authentication, authorization, and accounting."

23. A report in 2023 from the cyber intelligence firm Cyble noted that telecommunications companies in the U.S. are a target for hackers. The report found that most data breaches involve third-party vendors. These "can lead to . . . larger scale . . . supply-chain attacks and a greater number of impacted users and entities globally . . ."[12] So, whether the breach occurred through AT&T's systems or those of its vendors, AT&T was responsible for the protection of customers' PII.

24. AT&T recognized these very risks in public filings. Its 2023 Annual Report acknowledged the business risk of a cybersecurity incident and the need to manage third-party risk from vendors:

Network Providers and Devices, CISA.GOV, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PRO VIDERS_DEVICES_TLPWHITE.PDF (last visited Apr. 4, 2024).

[12] https://cyble.com/blog/u-s-telecommunications-companies-targeted-consumers-hit-hardest/?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=top#_ga=2.42536483.783648717.1711826278-1958601959.1709241562.

Risk Management and Strategy

We maintain a network and information security program that is reasonably designed to protect our information, and that of our customers, from unauthorized risks to their confidentiality, integrity, or availability. Our program encompasses the CSO and its policies, platforms, procedures, and processes for assessing, identifying, and managing risks from cybersecurity threats, including third-party risk from vendors and suppliers; and the program is generally designed to identify and respond to security incidents and threats in a timely manner to minimize the loss or compromise of information assets and to facilitate incident resolution.

We maintain continuous and near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. This security monitoring leverages tools, where available, such as near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trend analysis and predictive security alerting. We assess, identify, and manage risks from cybersecurity threats through various mechanisms, which from time to time may include tabletop exercises to test our preparedness and incident response process, business unit assessments, control gap analyses, threat modeling, impact analyses, internal audits, external audits, penetration tests and engaging third parties to conduct analyses of our information security program. We conduct vulnerability testing and assess identified vulnerabilities for severity, the potential impact to AT&T and our customers, and likelihood of occurrence. We regularly evaluate security controls to maintain their functionality in accordance with security policy. We also obtain cybersecurity threat intelligence from recognized forums, third parties, and other sources as part of our risk assessment process. In addition, as a critical infrastructure entity, we collaborate with numerous agencies in the U.S. government to help protect U.S. communications networks and critical infrastructure, which, in turn, informs our cybersecurity threat intelligence.

Cyberattacks impacting our networks or systems may have a material adverse effect on our operations.

Cyberattacks – including through the use of malware, computer viruses, distributed denial of services attacks, ransomware attacks, credential harvesting, social engineering and other means for obtaining unauthorized access to or disrupting the operation of our networks and systems and those of our suppliers, vendors and other service providers – could have a material adverse effect on our operations. Cyberattacks can cause equipment or network failures, loss of information, including sensitive personal information of customers or employees or proprietary information, as well as disruptions to our or our customers', suppliers' or vendors' operations, which could result in significant expenses, potential investigations and legal liability, a loss of current or future customers and reputational damage. As our networks evolve, they are becoming increasingly reliant on software to handle growing demands for data consumption. Cyberattacks against companies, including the Company and its suppliers and vendors, have occurred and will continue to occur and have increased in frequency, scope and potential harm in recent years. Further, the use of artificial intelligence and machine learning by cybercriminals may increase the frequency and severity of cybersecurity attacks against us or our suppliers, vendors and other service providers. Additionally, as cyberattacks become increasingly sophisticated, a post-attack investigation may not be able to ascertain the entire scope of the attack's impact. Extensive and costly efforts are undertaken to develop and test systems before deployment and to conduct ongoing monitoring and updating to prevent and withstand such attacks. While, to date, we have not been subject to cyberattacks that, individually or in the aggregate, have been material to our operations or financial condition, the preventive actions we take to reduce the risks associated with cyberattacks may be insufficient to repel or mitigate the effects of a major cyberattack in the future.

25. Further, AT&T has experienced data breaches before. Last year it reported that customer information of 9 million of its wireless users had been taken when a third-party marketing vendor was breached.[13] And in 2014, AT&T settled a Federal Communications Commission investigation into privacy violations for $25 million following the leak of about 280,000 U.S. customers' names and full or partial Social Security numbers.[14]

[13] https://www.cnet.com/tech/mobile/at-t-vendor-data-breach-exposed-9-million-customer-accounts/

[14] https://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html.

26. AT&T also knew or should have known of the risk of criminal breach of its information systems following high-profile data breaches in 2023 at telecommunications companies like Xfinity, T-Mobile, and other companies, which affected tens of millions of customers.

27. CISA advises that organizations take steps to prevent unauthorized access, such as: conducting regular vulnerability scanning on internet-facing devices; update and patch software to latest versions, especially for servers and software that processes internet data; disabling Server Message Block (SMB), an operating system network file sharing protocol that is used to spread malware or access sensitive data across a network; use best practices for Remote Desktop Protocol (RDP) as threat actors often first access networks when remote services are poorly secured; properly configure devices and ensure security features are enabled.[15] CISA also recommends that organizations use centrally managed antivirus software that automatically updates in order to protect all internet-connected devices, as well as putting in place a real-time intrusion detection system for malicious activity that may precede ransomware deployment.[16]

---

[15] https://www.cisa.gov/sites/default/files/publications/CISA_MSISAC_Ransomware%20Guide_S508C_.pdf at 4.

[16] *Id.* at 5.

28. Despite its awareness of the publicly available knowledge of the continued PII compromises and despite holding the PII of millions of customers, AT&T failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class members' PII.

29. Had AT&T used industry standard security measures, adequately invested in data security, and investigated cybersecurity issues promptly, unauthorized actors likely would not have gained access to its or its vendors' or partners' systems, thereby preventing or lessening the extent of the Data Breach.

Plaintiff's PII Has Value

30. Criminal actors highly value customer PII. Such information is continually traded on underground "dark web" marketplaces that cannot be accessed through standard web browsers. Personal information, bank details, payment card details, and online banking logins fetch prices in the tens to hundreds of dollars.[17]

[17] 1 Anita George, Your personal data is for sale on the dark web. Here's how much it costs, DIGITALTRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-webhow-much-it-costs/; Zachary Ignoffo, Dark Web Price Index 2021, PRIVACYAFFIARS.COM, https://www.privacyaffairs.com/dark-web-price-index-2021/ (Jun. 10, 2023). 23 For Sale in the Dark, VPN OVERVIEW, https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/ (last visited Jan. 17, 2024).

Criminals can also buy access to information from an entire company data breach for a few thousand dollars.[18]

31. Data that include PII sell for much higher on the black market. The kind of information likely exposed in the Data Breach is of much higher value than simple credit card information, which customers can change or close accounts.[19] By contrast the PII exposed in the Data breach cannot readily be changed—*e.g.*, addresses and Social Security numbers.

32. PII also sells on legitimate markets, an industry that is valued at hundreds of billions of dollars per year.[20] Customers themselves are able to sell non-public information directly to data brokers who aggregate the information for sale to marketers or others.[21] Consumers may also sell their web browsing histories to the Nielson Corporation for up to $50 annually.

---

[18] Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-theblack-market/ (July 27, 2015).

[19] *See* Jesse Damiani, Your Social Security Number Costs $4 on the Dark Web, New Report Finds, FORBES, https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-darkweb-new-report-finds/?sh=770cee3a13f1 (Mar. 25, 2020).

[20] Devan Burris, How grocery stores are becoming data brokers, CNBC, https://www.cnbc.com/2023/12/10/how-grocery-stores-are-becoming-databrokers.html#:~:text=In%202021%20the%20data%20broker,better%20idea%20of %20consumer %20trends. (Dec. 10, 2023, 12:00 PM).

[21] https://datacoup.com/#first-stop (last visited Jan. 17, 2024).

33. Because their PII has value, Plaintiff and Class members must take protective measures, for example, placing "alerts" with credit reporting agencies and monitoring credit report activity, as AT&T's online notice instructs the Data Breach victims to do.

Allegations Relating to Plaintiff

34. Plaintiff Terri Lynn Hodge resides in Gilmer, Texas, and has been an AT&T wireless customer since 2004.

35. In connection with obtaining services, Ms. Hodge was required to provide highly sensitive personal information, such as her contact information, date of birth, and Social Security number. AT&T also prompted Ms. Hodge to create login credentials to access her accounts.

36. AT&T shared Ms. Hodge's information with third-party partners in the course of its business. AT&T was obligated to verify those partners' data security practices because they stored the information AT&T collected.

37. Ms. Hodge became aware of the data breach on or around April 1, 2024, via an e-mail notice that AT&T sent her. The notice recommended that she take certain actions like resetting her account passcode, monitoring her credit reports, and signing up for fraud alerts.

38. As a result of the Data Breach, Ms. Hodge received a notification from a credit monitoring service that her PII, including her name and contact information,

had appeared on the dark web. Ms. Hodge also spent time researching the breach and reviewing her credit reports and bank accounts for evidence of unauthorized activity, which she will continue to do so indefinitely.

39. Because AT&T continues to store and share Ms. Hodge's and Class Members' PII for use in its business, they have a continuing interest in ensuring their PII is kept safe from further unauthorized access.

AT&T Did Not Comply with Federal Law and Regulatory Guidance

40. The United States government issues guidelines for businesses that store sensitive data to help them minimize the risks of a data breach. The FTC publishes guides for businesses about the importance of reasonable data security practices.[22] One of its publications sets forth data security principles and practices for businesses to protect sensitive data.[23] The FTC tells businesses to (a) protect the personal information they collect and store; (b) dispose of personal information it no longer needs; (c) encrypt information on their networks; (d) understand their network's vulnerabilities; (e) put policies in place to correct security problems. The FTC recommends businesses use an intrusion detection system, monitor networks

[22] Start with Security: A Guide for Business, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 17, 2024).
[23] Protecting Personal Information: A Guide for Business, FTC.ORG, https://www.ftc.gov/businessguidance/resources/protecting-personal-informationguide-business (last visited Jan. 17, 2024).

for large, outgoing data transmissions, monitor incoming traffic for unusual activity, and make a plan in case a breach occurs.[24]

41. Further, the FRC tells organizations to limit access to sensitive data, require the use of complex passwords on networks, use industry-tested security methods; and verify the use of reasonable security measures by third-party service providers.[25]

42. The FTC brings enforcement actions against businesses that fail to reasonably protect customer information. The Commission treats the failure to use reasonable care and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders issued in these actions state the measures required for businesses to meet their data security obligations.[26]

43. AT&T knew of its obligation to implement and use reasonable measures to protect customers' PII. AT&T nonetheless failed to comply with those recommendations and guidelines, which if followed would have prevented the Data

---

[24] *Id.*

[25] 3 Start with Security: A Guide for Business, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 17, 2024).

[26] FTC, Privacy and Security Enforcement, FTC.GOV, https://www.ftc.gov/newsevents/mediaresources/protecting-consumerprivacy/privacy-security-enforcement (last visited Jan. 17, 2024).

Breach. This failure to reasonably protect against unauthorized access to PII is an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

44. AT&T's failure to protect customer PII suggests its failure to comply fully with standard cybersecurity practices such as network segmentation, rate limiting, proper firewall configuration, secure credential storage, user-activity monitoring, encryption, data-loss prevention, intrusion detection and prevention, and managerial control over vendors' cybersecurity practices.

The Data Breach Caused Its Victims Harm

45. As a result of the Data Breach, hackers can now commit identity theft, financial fraud, and other fraud against Plaintiff and Class members, given the stolen PII's sensitive nature.

46. Plaintiff and Class members therefore have suffered injury and face an imminent, substantial risk of further injuries like identity theft and related cybercrimes. Plaintiff's and Class members' PII have been published to the Dark Web for misuse by cybercriminals.

47. The PII likely exposed in the Data Breach is highly valuable and sought after on underground markets for use in committing identity theft and fraud. Malicious actors use this data to access bank accounts, credit cards, and social media accounts, among other things. They may also use the PII to open new financial or utility accounts, seek medical treatment using victims' insurance, file fraudulent tax

returns, seek and obtain government benefits or government IDs, or create new identities for use in committing frauds. Because victims of breaches can become less diligent in account monitoring over time, bad actors may wait years before using the PII, or they may re-use it to commit several cybercrimes.

48. Even where individuals receive reimbursement for resulting financial losses, they are not made whole again because of the significant time and effort required to do so. The Government Accountability Office reported that stolen data may not be used to commit identity theft for more than a year after it is obtained. And fraudulent use of data may continue for years after its sale or publication. It concluded that studies that try to measure harms from data breaches "cannot necessarily rule out all future harm."[27]

49. The Identity Theft Resource Center's 2021 survey reported that victims of identity theft reported suffering negative experiences and emotional harms: anxiety (84%); feelings of violation (76%); rejection for credit or loans (83%); financial related identity problems (32%); resulting problems with family members (32%); feeling suicidal (10%).[28]

[27] http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 17, 2024).
[28] 2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces, https://www.idtheftcenter.org/wpcontent/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Jan. 17, 2024).

50. Physical harms also result from identity theft. A similar survey found that victims suffered resulting physical symptoms: sleep disturbances (48.3%); inability to concentrate / lack of focus (37.1%); inability to work because of physical symptoms (28.7%); new physical illnesses including stomach problems, pain, and heart palpitations (23.1%); starting or relapsing into unhealthy or addictive behaviors (12.6%).[29]

51. Unauthorized disclosure of sensitive PII also reduces its value to its rightful owner, as recognized by courts as an independent source of harm.[30]

52. Even consumers who have been victims of previous data breaches are injured when their data is stolen and traded. Each data breach increases the likelihood that the victim's personal information will be exposed on the dark web to more individuals who are looking to misuse it.

---

[29] Identity Theft: The Aftermath 2017, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Apr. 5, 2024).

[30] See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

53. Because of these injuries resulting from the Data Breach, Plaintiff and Class members suffer and continue to suffer economic loss and actual harm, including:

- disclosure or confidential information to a third party without consent;
- loss of the value of explicit and implicit promises of data security;
- identity fraud and theft; anxiety, loss of privacy, and emotional distress;
- the cost of detection and prevention measures for identity theft and unauthorized financial account use;
- lowered credit scores from credit inquiries; unauthorized charges;
- loss of used of financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amounts they were permitted to obtain from accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- costs of credit monitoring, identity theft production services, and credit freezes;
- costs associated with loss of time or productivity or enjoyment of one's life from the time required to mitigate and address consequences and future consequences of the Data Breach, such as searching for

fraudulent activity, imposing withdrawal and purchase limits, as well as the stress and nuisance of Data Breach repercussions;

- imminent, continued, and certainly impending injury flowing from the potential fraud and identity theft posed by the unauthorized possession of data by third parties.

54. Plaintiff and Class members place a significant value on data security. About half of consumers consider data security to be a main or important consideration in their purchasing decision and would be willing to pay more to work with those with better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[31]

55. Telecommunications businesses with strong data security practices are viewed more favorably by consumers and can ask higher prices than those who do not. For this reason, had customers known that AT&T did not protect and store PII adequately or monitor the data security of third-party partners adequately, they would not have contracted with AT&T or would have paid significantly less. Plaintiff and Class members therefore did not receive the benefit of their bargain with AT&T after having paid for the value of services they did not receive.

[31] https://web.archive.org/web/20230628100935/https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf, at p.14 (last visited Apr. 5, 2024).

56. Plaintiff and Class members have a direct interest in AT&T's promises and duties to protect their PII—*i.e.*, that AT&T not increase their risk of identity theft and fraud. AT&T failed on these promises and duties, and Plaintiff and Class members therefore seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm from AT&T's wrongful conduct. Plaintiff and Class members seek this remedy to restore themselves as close to the same position as they would have occupied but for AT&T's failure to protect Plaintiff's and Class members' PII.

57. Plaintiff and Class members also seek to recover the value of the unauthorized access to their PII that AT&T's wrongful conduct permitted. These damages are analogous to the remedies for unauthorized use of intellectual property. Unauthorized use of or access to PII is like another's use of patented or protected technology. Although unauthorized use of that technology does not diminish the rights-holder's ability to use the same, the reasonable use value may generally be recovered—a "reasonable royalty" from the infringer. This is true even though the infringer's use did not interfere with the owner's use and the owner would not have otherwise licensed that use. The same royalty or license measure of damages is warranted here under the principles of common law damages, which authorize recovery of rental or use value. This is appropriate here because (a) Plaintiff and Class members have a protectible property interest in their PII; (b) rental value is the

minimum damages measure for the unauthorized use of personal property; and (c) rental value is established according to market value.

58. AT&T's delay in disclosing the Data Breach and notifying the victims also caused harm to Plaintiff and Class members. Had AT&T not ignored the 2021 claims that its customers' PII was being auctioned on the dark web and instead conducted a prompt and adequate investigation, Plaintiff's and Class members' PII likely would not have been exposed years later. AT&T's decision not to investigate or attempt to discover key facts is important because the affected individuals may take different precautions depending on the severity and imminence of the perceived risk. AT&T's delay therefore prevented victims from mitigating their harms.

59. Plaintiff and Class members have an interest in ensuring that their PII is secure and not subject to further theft, as AT&T continues to hold that PII.

CLASS ACTION ALLEGATIONS

60. Plaintiff seeks relief in her individual capacity and as representative of others similarly situated. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of herself and the Class, which is defined as: All individuals whose personal information was compromised in the Data Breach announced by AT&T in March 2024 (the "Class").

61. The following are excluded from the Class: AT&T; its officers, directors, or employees; any entity in which AT&T has a controlling interest; and

any affiliate, legal representative, heir, or assignee of AT&T. Also excluded from the Class are any federal, state, or local governmental entities; any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

62. Class Identity: The Class members are readily identifiable and ascertainable. AT&T and/or its affiliates possess the information to identify and contact class members.

63. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. AT&T's disclosures reveal that the Class contains more than 73 million individuals whose PII was compromised.

64. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members had their PII compromised in the Data Breach and were harmed as a result.

65. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. She has no known interest antagonistic to those of the Class and her interests are aligned with Class members' interests. Plaintiff was subject to the same Data Breach as Class members, suffered similar harms, and faces similar threats from the Data Breach. Plaintiff has retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

66. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. Common questions will predominate over any questions affecting only individual class members. These include:

- Whether AT&T owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;
- Whether AT&T owed Plaintiff and Class members a duty to exercise due care in partnering with third parties with whom it shares PII and in conducting oversight of third parties to ensure their adequate data protection to protect that PII in the course of carrying out their partnership;
- Whether AT&T was negligent in connection with the monitoring and/or protection of Plaintiff's and Class members' PII;
- Whether AT&T received a benefit without proper restitution making it unjust for AT&T to retain the benefit without giving compensation;
- Whether AT&T violated its duty to implement reasonable security procedures and practices to protect Plaintiff's and Class members' PII;

- Whether AT&T's breach of its duty to exercise due care and conduct oversight of third parties' data security practices directly and/or proximately caused damages to Plaintiff and Class members;
- Whether AT&T's breach of its duty to implement reasonable security procedures and practices directly and/or proximately caused damages to Plaintiff and Class members;
- Whether AT&T adequately fixed the problems in its information systems that enabled the Data Breach;
- Whether Plaintiff and Class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of PII;
- Whether AT&T provided timely notice of the Data Breach to Plaintiff and Class members; and
- Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

67. AT&T has engaged in a common course of conduct and Plaintiff and Class members have been similarly impacted because of its failure to reasonably secure its customers' PII and also because of its failure to alert its affected customers to the Data Breach in a timely manner.

68. Superiority: A class action is superior to other methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or other piecemeal litigation. The cost of litigating individual claims is prohibitively high and would create a risk of inconsistent adjudications as to individual class members and would risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in maintaining this as a class action under the applicable rules.

CAUSES OF ACTION

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

69. Plaintiff repeats and realleges every allegation in the preceding paragraphs.

70. Defendant AT&T required the PII of Plaintiff and Class members as a condition to receiving services. AT&T collected and stored this PII for commercial gain. AT&T also collected, stored, and through its partnerships with third-party vendors, shared the data with those vendors for providing AT&T's services, as well as for commercial gain.

71. In partnering with third-party vendors, AT&T owed Plaintiff and Class members a duty to supervise and ensure the vendors maintained adequate data

security to protect Plaintiff's and Class members' PII within its control for carrying out the partnership consistent with industry standards. AT&T owed Plaintiff and Class members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access, which duty AT&T acknowledged in its policies describing its handling of PII and promising not to disclose PII without authorization.

72. AT&T owed Plaintiff and Class members a duty of care to provide adequate data security, consistent with industry standards, and to ensure that it and its vendors' systems and networks adequately protected the PII.

73. AT&T owed a duty of care to Plaintiff and Class members to timely remedy any flaws within its systems so as to reduce the risk that Plaintiff and Class members' PII would be compromised.

74. AT&T's duty to use reasonable care in protecting Plaintiff's and Class Members' PII arose from the parties' relationship, and from the common law and federal law, including the FTC regulations described above, and AT&T's policies and promises regarding privacy and data security.

75. AT&T knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location for carrying out the partnership's business, of its vendors' vulnerability to network attacks, and of the importance of adequate security.

76. AT&T breached its duty to Plaintiff and Class members, as described herein, including by:

- failing to use reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' PII;
- failing to ensure its vendors used adequate security systems, protocols, and practices to sufficiently protect Plaintiff's and Class members' PII;
- failing to supervise its vendors with respect to their data security systems, protocols, and practices when it knew or should have known they were inadequate;
- failing to comply with industry-standard data security measures;
- failing to comply with its own privacy policies;
- failing to comply with regulations protecting Plaintiff's and Class members' PII;
- failing to adequately monitor, evaluate, and ensure the security of their vendors' network and systems;
- failing to timely recognize that the PII had been compromised; and
- failing to timely and adequately disclose the Data Breach.

77. Plaintiff's and Class members' PII would not have been compromised but for AT&T's wrongful and negligent breach of its duties.

78. AT&T's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access, copying, and exfiltrating of PII by unauthorized third parties. Given that telecommunications businesses are prime targets for hackers, Plaintiff and Class members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by AT&T.

79. It was also foreseeable that AT&T's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and Class members.

80. As a direct and proximate result of AT&T's conduct, Plaintiff and Class members have and will suffer damages including: (i) the loss of use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic

and non-economic losses; (vii) the continued risk to their PII, which remains in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

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

81. Plaintiff repeats and realleges every allegation in the preceding paragraphs.

82. Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as AT&T, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

83. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

84. AT&T violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. AT&T's conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable

consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and Class members. AT&T further violated Section 5 of the FTC Act by willfully ignoring earlier cybersecurity issues in pursuit of financial gain. Indeed, had AT&T recognized the cybersecurity issues in 2021, it would have likely affected AT&T's bottom line.

85. AT&T's violations of Section 5 of the FTC Act constitute negligence *per se.*

86. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

87. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class members. As a direct and proximate result of AT&T's negligence *per se*, Plaintiff and Class members sustained actual losses and damages as alleged herein. Plaintiff and Class members alternatively seek an award of nominal damages.

THIRD CAUSE OF ACTION
Breach of Contract
(*On Behalf of Plaintiff and the Class*)

88. Plaintiff repeats and realleges every allegation in the preceding paragraphs.

89. AT&T disseminated a "Privacy Notice" to its customers that constitutes an agreement between AT&T and persons who provided their PII to AT&T, including Plaintiff and Class members.

90. Plaintiff and Class members formed a contract with AT&T and complied with all obligations under such contract when they provided PII to AT&T subject to the Privacy Notice.

91. AT&T promised in its Privacy Notice that it "work[s] hard to safeguard [customers'] information using technology controls and organizational controls." AT&T further instructed that it "limit[s] access to personal information to the people who need access for their jobs." AT&T also promises that when customers' PII is no longer needed for "business, tax or legal purposes," that it will "destroy it by making it unreadable or indecipherable." And in the event of a data breach, AT&T will "notify [customers] as required by law."

92. AT&T breached its agreements with Plaintiff and Class members when AT&T allowed for the disclosure of Plaintiff's and Class members' PII without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Privacy Notice, as well as when it failed to maintain the confidentiality of Plaintiff's and Class members' PII.

93. As a direct and proximate result of these breaches, Plaintiff and Class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class members alternatively seek an award of nominal damages.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

94. Plaintiff repeats and realleges every allegation in the preceding paragraphs and asserts this claim in the alternative to her breach of contract claim to the extent necessary.

95. Plaintiff and Class members were required to provide their PII to AT&T as a condition to receiving AT&T's services.

96. As part of these transactions, AT&T agreed to safeguard and protect the PII of Plaintiff and Class members. Implicit in these transactions between AT&T and Class members was the obligation that AT&T would use the PII for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

97. Additionally, AT&T implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or access.

98. Plaintiff and Class members entered into implied contracts with the reasonable expectation that AT&T's data security practices and policies, including adequate managerial supervision of vendors' data security, were reasonable and consistent with industry standards. Plaintiff and Class members believed that AT&T would use part of the monies paid to AT&T under the implied contracts to fund adequate and reasonable data security practices to protect their PII.

99. Plaintiff and Class members would not have provided and entrusted their PII to AT&T or would have paid less for AT&T's services in the absence of the implied contract between them and AT&T. The safeguarding of Plaintiff's and Class members' PII was critical to realizing the intent of the parties.

100. The nature of AT&T's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and Class members' PII in order to prevent harm and prevent present and continuing increased risk.

101. AT&T breached its implied contract with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII, which was compromised as a result of the Data Breach.

102. As a direct and proximate result of AT&T's breaches, Plaintiff and Class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class members alternatively seek an award of nominal damages.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

103. Plaintiff repeats and realleges every allegation in the preceding paragraphs.

104. Plaintiff and Class members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by AT&T and which was stolen in the Data Breach. This information has independent value.

105. Plaintiff and Class members conferred a monetary benefit on AT&T in the form of payments for its services, including those paid indirectly by Plaintiff and Class members to AT&T.

106. AT&T appreciated and had knowledge of the benefits conferred upon them by Plaintiff and Class members.

107. The price for wireless services that Plaintiff and Class members paid (directly or indirectly) to AT&T should have been used by AT&T, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures, including adequate managerial supervision of vendors' data security.

108. Likewise, in exchange for receiving Plaintiff's and Class members' valuable PII, which AT&T was able to use for its own business purposes and which provided actual value to AT&T, AT&T was obligated to devote sufficient resources

to reasonable data privacy and security practices and procedures, including adequate managerial supervision of vendors' data security.

109. As a result of AT&T's conduct, Plaintiff and Class members suffered actual damages as described herein. Under principles of equity and good conscience, AT&T should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds they received from Plaintiff and Class members, including damages equaling the difference in value between services that included implementation of reasonable data privacy and security practices that Plaintiff and Class members paid for and the services without reasonable data privacy and security practices that they actually received.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

110. Plaintiff repeats and realleges every allegation in the preceding paragraphs.

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

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

113. AT&T still possesses PII pertaining to Plaintiff and Class members and continues to share this PII with its vendors, which means Plaintiff's and Class members' PII remains at risk of further breaches because AT&T's data security measures remain inadequate. Plaintiff and Class members continue to suffer injuries as a result of the compromise of their PII and remain at an imminent risk that additional compromises of their PII will occur in the future.

114. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) AT&T's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) AT&T must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry standard security measures, including, but not limited to, those listed at (2)(ii)(A)-(I), *infra*, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and Class members' PII if it is no longer necessary to perform essential business functions so

that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

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

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

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

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

E. Purging, deleting, and destroying in a reasonable and secure manner PII not necessary to perform essential business functions;

F. Conducting regular database scanning and security checks;

G. Conducting regular employee education regarding best security practices;

H. Implementing multi-factor authentication and Principal of Least Privilege (POLP) to combat system-wide cyberattacks; and

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

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representative, and Plaintiff's counsel as Class Counsel;

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

C. That the Court award Plaintiff and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each cause of action as allowed by law in an amount to be determined at trial;

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

E. 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;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

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

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in this action.

Date: April 6, 2024.

Respectfully submitted,

/s/ J. Cameron Tribble
J. Cameron Tribble
Georgia Bar No. 754759
Roy E. Barnes
Georgia Bar No. 039000
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Tel: 770-227-6375
roy@barneslawgroup.com
ctribble@barneslawgroup.com

David M. Berger *
Linda P. Lam*
GIBBS LAW GROUP LLP
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: 510-350-9700
dmb@classlawgroup.com
lpl@classlawgroup.com

**Pro hac vice forthcoming*