UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

RYAN UNRUH and CHRISTOPHER ISBELL, 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 Ryan Unruh and Plaintiff Christopher Isbell ("Plaintiffs"), by and through the undersigned counsel, bring this class action against Defendant AT&T Mobility LLC and Defendant AT&T, Inc. (collectively, "AT&T" or "Defendants"), on behalf of themselves and all other similarly situated. Plaintiffs make the following allegations based on the personal knowledge as to their own action and on information and belief as to all other matters:

NATURE OF THE ACTION

1. Nearly three years ago, AT&T – the country's largest wireless carrier – learned that a well-known threat actor claimed to be selling a database containing the personal information of over 70 million AT&T customers. This information

included customers' names, addresses, phone numbers, Social Security numbers, and dates of birth. But instead of investigating the source and cause of the massive breach, AT&T denied the allegations, ignored the issue, and continued with operations. AT&T told one media outlet that "the information that appeared in an internet chat room does not appear to have come from our systems."[1] And when questioned about its vendors, AT&T chose not to speculate: "Given this information did not come from us, we can't speculate on where it came from or whether it is valid."[2] AT&T attempted to fully wash its hands of the disaster.

2. Almost three years later, the same customer data from 2021 is no longer just for sale; it has been fully exposed on the Dark Web. And after years of denial, AT&T has changed its tune. AT&T finally admitted that approximately 73 million former and current AT&T customers' personal and sensitive information was released onto the Dark Web (the "Data Breach"). According to AT&T, customers' impacted information included a combination of their "full name, email address, mailing address, phone number, social security number, date of birth, and AT&T account number and passcode" (collectively, "PII"), which AT&T collected as a

---

[1] Lawrence Abrams, *AT&T denies data breach after hacker auctions 70 million user database*, BLEEPINGCOMPUTER (Aug. 20, 2021, 9:43 AM), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/.

[2] *Id.*

condition for use of its services. This recent revelation marks a concerning turn of events.

3. Equally troubling is that AT&T still appears clueless as to the source of the breach. One would hope that – in nearly three years – a telecom giant like AT&T would have conducted a "robust investigation" into the data leak to determine who was responsible, where the data originated from, which customers were impacted, how the Data Breach occurred, and other key factors. But it did not. Had it done so, the 73 million customers could have attempted to adequately protect themselves. Instead, AT&T remained willfully blind.

4. This Data Breach and resulting injuries occurred because AT&T failed to implement reasonable security procedures and practices (including failing to exercise appropriate managerial control over third-party partner's data security), failed to disclose material facts surround its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

5. As a result of AT&T's failure to protect the PII it was entrusted to safeguard, Plaintiffs and class members now face a significant risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

6. Plaintiff Ryan Unruh is a citizen and resident of Kansas whose PII was compromised from AT&T.

7. Plaintiff Christopher Isbell is a citizen and resident of Florida whose PII was compromised from AT&T.

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

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

JURISDICTION AND VENUE

10. 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 at least 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.

11. 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.

12. This Court has jurisdiction over Defendant AT&T Inc. because AT&T has committed acts with the Northern District of Georgia giving rise to this action and has established minimum contacts with 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 Inc. 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.

13. 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

Defendants' Privacy Practices

14. AT&T is the largest wireless carrier in the United States, with 241.5 million subscribers as the end 2023. In connection with providing its wireless services, AT&T requires consumers to provide personal information, including but not limited to names, addresses, Social Security numbers, and dates of birth. As a

result, when consumers contract AT&T's services, their highly sensitive PII is stored on AT&T's network servers.

15. Given the amount and sensitive nature of the data it collects, AT&T maintains policies explaining its privacy practices handling consumers' personal information. Through these policies, AT&T represents to consumers and the public that it possesses robust security features to protect PII and it they their responsibility to protect PII seriously. For example, AT&T claims that it "work[s] hard to safeguard [customers'] information using technology controls and organizational controls."[3] AT&T further instructs that it "limit[s] access to personal information to the people who need access for their jobs."[4] 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."[5] And in the event of a data breach, AT&T will "notify [customers] as required by law."[6]

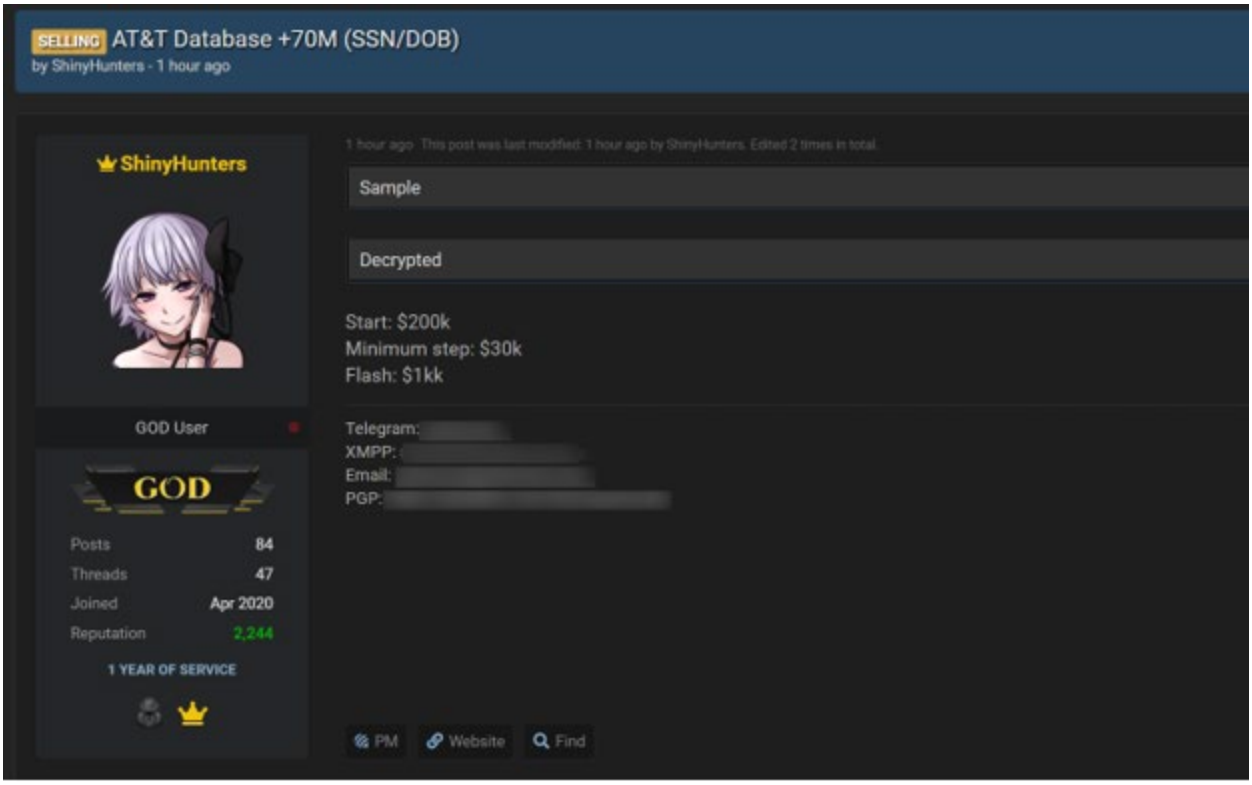
16. Given AT&T's avowed experience in its field handling highly sensitive personal information, it understood the need to protect consumers' PII and prioritize data security.

---

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

Hackers Auction PII of Over 70 Million AT&T Customers in August 2021

17. AT&T learned of the Data Breach nearly three years ago. In August 2021, ShinyHunters, a notorious hacking group, offered "AT&T Database +70M (SSN/DOB)" on a hacker forum and marketplace.[7] ShinyHunters offered the database for a starting price of $200,000 with incremental increases of $30,000 and provided a same of decrypted values. The hackers stated they would sell immediately for $1 million.



[7] 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/.

18. Once learning of ShinyHunters claims, AT&T represented that the data did not appear to come from its servers.[8] When pressed about whether the information could have been stolen from a third-party partner, AT&T stated that it could not "speculate on where it came from or whether it is valid."[9]

19. Continuing with its willfully blind attitude, AT&T denied responsibility, ignored the disaster, and continued operations.

The Data Breach

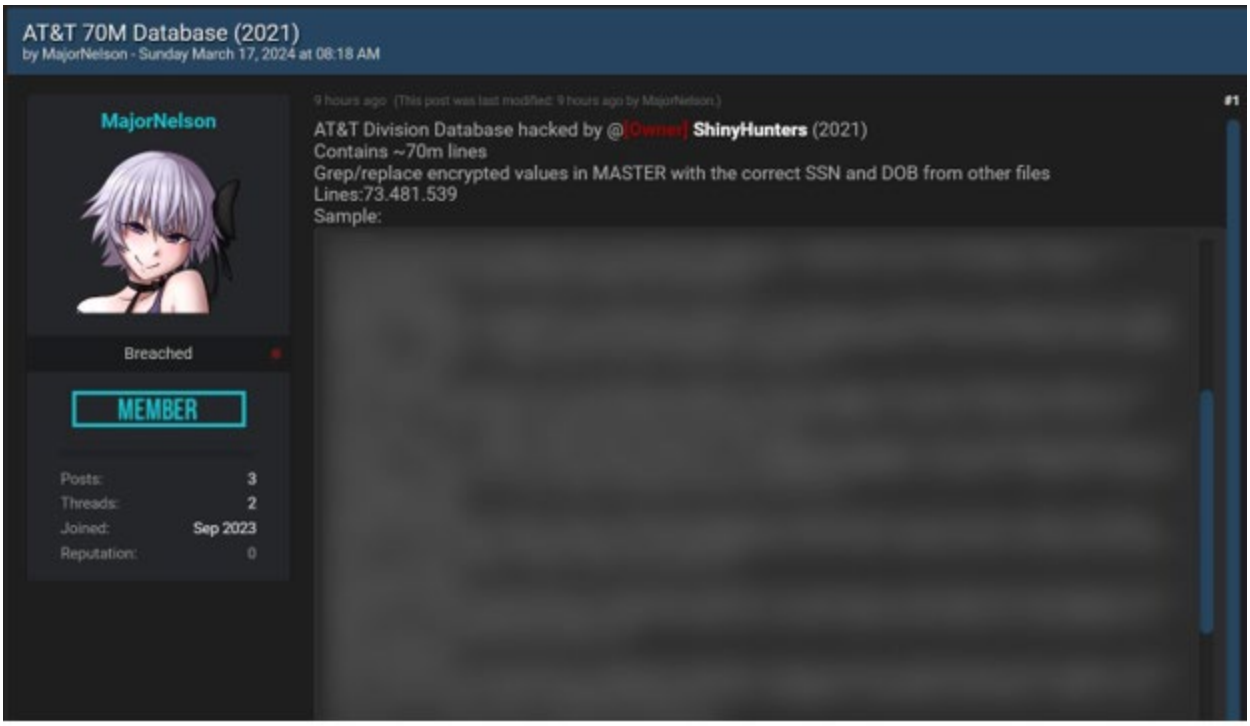
20. Nearly three years later, another threat actor has claimed to have leaked the same data ShinyHunters attempted to sell in August 2021. On March 17, 2024, MajorNelson leaked the database obtained by ShinyHunters for free on a hacking forum.[10] This data includes names, addresses, mobile phone numbers, decrypted birth dates and Social Security numbers, and other information. BleepingComputer, a data breach media outlet, reviewed and confirmed the leaked data with several impacted individuals.

---

[8] Lawrence Abrams, *AT&T denies data breach after hacker auctions 70 million user database*, BLEEPINGCOMPUTER (Aug. 20, 2021, 9:43 AM), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/.

[9] *Id.*

[10] Lawrence Abrams, *AT&T says leaked data of 70 million people is not from its systems*, BLEEPINGCOMPUTER (Mar. 17, 2024, 7:24 PM), https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/.



21. With its feet to the fire, AT&T finally acknowledged the legitimacy of the leaked customer data:

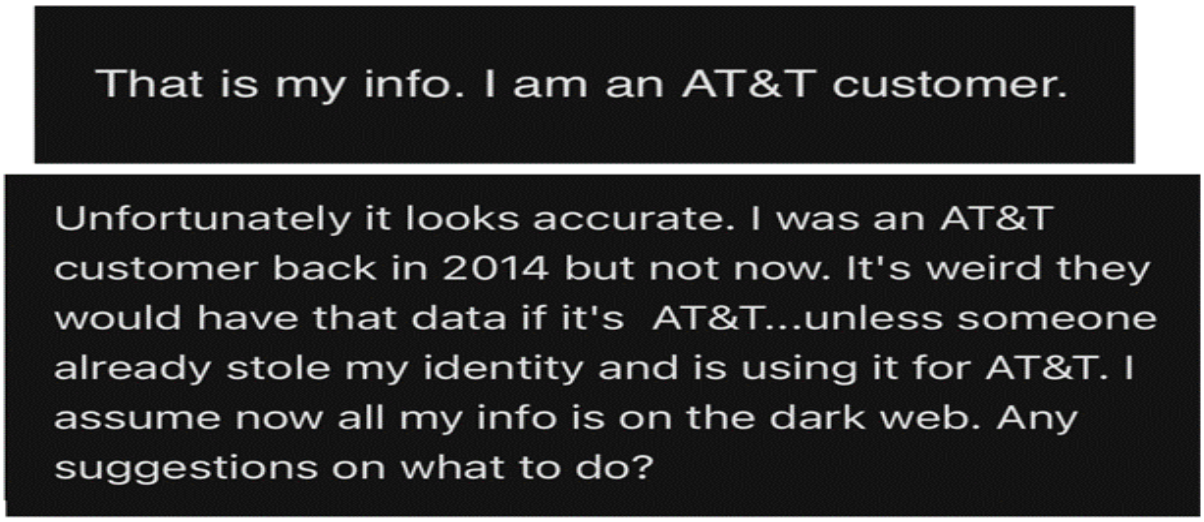
> AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance 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.

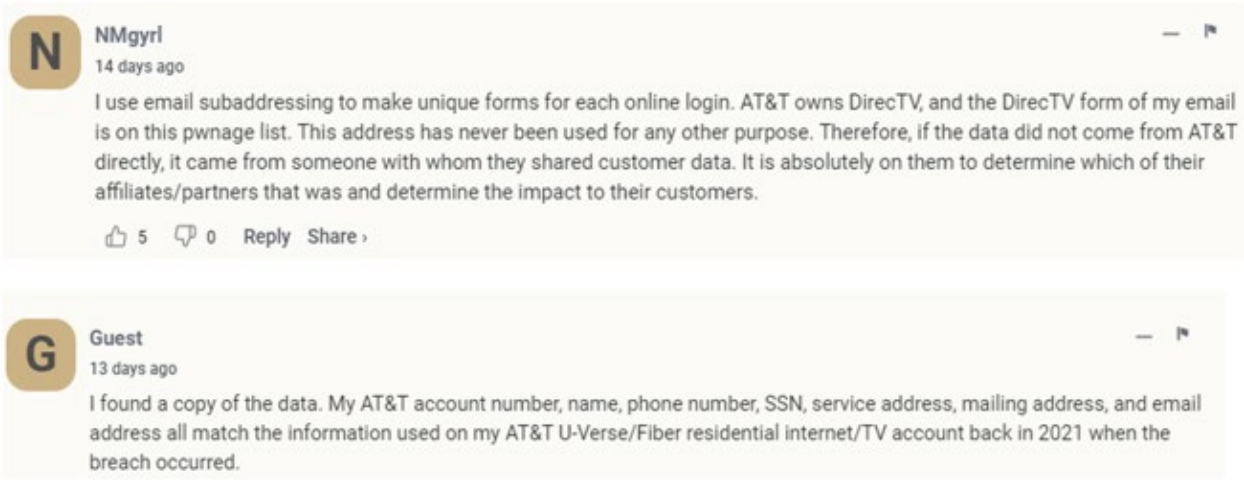
22. Experts have connected the August 2021 auctioned information to the Data Breach. Troy Hunt, a cybersecurity researcher specializing in the leak of consumer data,[11] concluded that the data "closely resembles a similar data breach that surfaced in 2021 but which AT&T never acknowledged…"[12] Similar to BleepingComputer, Hunt also verified the posted information with his 4.8 million subscribers, which confirmed that approximately 153,000 of them are part of the data set.[13] He also directly contacted potential victims and asked them to confirm whether their data was accurate and whether they happened to be an AT&T customer. Below are some of the responses:

---

[11] Matt O'Brien, *Have you been 'pwned' in a adata breach? Troy Hunt can tell*, AP (Dec. 5, 2017, 9:23 AM), https://apnews.com/article/739a98e040034eb79be4f951e72d52f8.
[12] https://apnews.com/article/att-data-breach-dark-web-passcodes-fbef4afe0c1deec9ffb470f2ec134f41
[13] https://www.troyhunt.com/inside-the-massive-alleged-att-data-breach/



23. Commentators on the article also noted that their stolen information appeared to have originated with AT&T:



24. Piecing together AT&T's negligence is not a difficult task. The AT&T database that was originally offered for sale in 2021 was published on the Dark Web for free almost three years later. And within those three years, AT&T has still not determined whether its systems were impacted or whether the data originated from

a third-party partner. Had AT&T took the 2021 allegations as seriously as it does collecting payment for its services, then it would have "launched a robust investigation supported by internal and external cybersecurity experts" years ago. Instead, what did AT&T do during those interim years? Nothing.

The Data Breach was Foreseeable and Preventable

25. Following the Data Breach, AT&T stated that it takes "cybersecurity very seriously and privacy is a fundamental commitment at AT&T."[14]

26. But AT&T, like any company of its size that stores massive amounts of sensitive PII, should have had robust protections in place to detect and terminate a successful intrusion long before access and exposure of customer data. AT&T also should have exercised appropriate managerial control over their third-party partners' data security when it knew these partners stored its customers' PII in the course of carry out the business of their partnership. AT&T's failure to prevent the breach is inexcusable given its knowledge that it and its affiliates are prime targets for cyberattacks.

27. In 2022, the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) coauthored the joint Cybersecurity Advisory explicitly highlighting

[14] https://www.att.com/support/article/my-account/000101995?bypasscache=1/?source=EPcc000000000000U.

"[t]elecommunications and network service provider targeting" by cyber actors.[15] The Advisory explains how cyber actors exploit and access telecommunication organizations and network service providers though the use of open-source tools "that allows for the scanning of IP addresses for vulnerabilities." Once these cyber actors gain an initial foothold, they identify "critical users and infrastructure including systems critical to maintaining the security of authentication, authorization, and accounting."

28. In addition to the Advisory, a 2023 report from cyber intelligence firm Cyble noted that U.S. telecommunications companies are a lucrative target for hackers. According to the study, the majority of data breaches stem from third-party vendors. "These third-party breaches can lead to a larger scale supply-chain attacks and a greater number of impacted users and entities globally…"[16] Thus, whether the

---

[15] *People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices,* CISA.GOV, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF (last visited Apr. 1, 2024).

[16] 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

data breach occurred through AT&T's own systems or its third-party vendors, AT&T was responsible for the protection of customers' PII.

29. And AT&T recognized these risks in its own regulatory filings. For instance, in its 2023 Annual Report, AT&T acknowledged the business risk of suffering a cyber security incident and the need to manage third-party risk from vendors:

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.

30. Aside from warnings from federal regulatory agencies and cyber intelligence firms, AT&T is no stranger to data breaches. Just a year ago, AT&T

notified 9 million wireless customers that their customer information had been accessed in a breach of a third-party marketing vendor.[17] And in 2014, AT&T settled a Federal Communications Commission investigation into privacy violations for $25 million. That investigation stemmed from the exposure of about 280,000 U.S. customers' names and full or partial Social Security numbers.[18]

31. If not through its own history, AT&T surely understood the risk from its competitors. Considering recent high profile data breaches at other telecommunications companies, such as Xfinity (36,000,000 impacted, announced December 2023); T-Mobile (37,000,000 impacted, announced January 2023); and US-Cellular (52,000 impacted, announced March 2023), among others, AT&T knew or should have known that its data and consumers' PII would be, or had already been, targeted by cybercriminals.

32. To prevent unauthorized access, CISA encourages organizations to:

- Conduct regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;

[17] https://www.cnet.com/tech/mobile/at-t-vendor-data-breach-exposed-9-million-customer-accounts/
[18] https://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html

- Regularly patch and update software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensure devices are properly configured and that security features are enabled;
- Employ best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disable operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[19]

33. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[20]

---

[19] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf at 4.
[20] *Id.* at 5.

34. Consequently, AT&T knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if their data security system was breached, including the significant costs that would be imposed on customers as a result of a breach.

35. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of customers, AT&T failed to use reasonable care in maintaining the privacy and security of the PII of Plaintiffs and Class members.

36. Had AT&T implemented industry standard security measures, adequately invested in data security, and promptly investigated cybersecurity issues, unauthorized parties likely would not have been able to access AT&T's or its third-party vendors' systems and the Data Breach would have been prevented or much smaller in scope.

Value of PII

37. The PII of consumers remains of high value to criminals, as evidenced by the continued sale and trade of such information on underground markets found on the "dark web"— which is a part of the internet that is intentionally hidden and inaccessible through standard web browsers.

38. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200,

and bank details have a price range of $50 to $200.[21] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23] Other sources show sensitive private information selling for as much as $363 per record.[24]

39. Data sets that include PII demand a much higher price on the black market. For example, the information likely exposed in the Data Breach is significantly more valuable than the loss of, for example, credit card information in

---

[21] 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-web-how-much-it-costs/.

[22] 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/anonymous-browsing/in-the-dark/ (last visited Jan. 17, 2024).

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

a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[25] The information likely disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

40. There is also an active and robust *legitimate* market for PII. In 2021, the data brokering industry alone was valued at $319 billion.[26] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[27] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[28]

41. Because their PII has independent value, Plaintiffs and Class members must take measures to protect it including by, as AT&T's online notice instructs, placing "alerts" with credit reporting agencies, changing passcodes, and reviewing

---

[25] 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-security-number-costs-4-on-the-darkweb-new-report-finds/?sh=770cee3a13f1 (Mar. 25, 2020).

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

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

[28] *Nielsen Computer & Mobile Panel, Frequently Asked Questions,* NIELSEN, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 17, 2023).

and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

Allegations Relating to Plaintiff Ryan Unruh

42. Plaintiff Ryan Unruh lives and resides in Overland Park, Kansas and has been a customer of AT&T for his personal and business accounts since 2014.

43. In connection with obtaining AT&T's services, Mr. Unruh was required to provide highly sensitive personal information, such as his contact information, date of birth, Social Security number, and so on. AT&T also prompted Mr. Unruh to create login credentials to access his accounts.

44. In the regular course of business, AT&T shared Mr. Unruh's information with several third-party partners whom AT&T was obligated to verify their data security practices because those third parties stored the information AT&T collected.

45. Mr. Unruh became aware of the data breach on April 1, 2024 and reviewed AT&T's online notice. The online notice recommends that customers take certain actions like resetting account passcodes and monitoring credit reports for activity and to detect errors. Furthermore, the online notice recommends that customers place a "fraud alert" on their credit report to detect any possible misuse of personal information.

46. As a result of the Data Breach, Mr. Unruh has spent time and effort researching the breach and reviewing his financial statements for evidence of unauthorized activity, which he will continue to do indefinitely.

47. Mr. Unruh also suffered emotional distress knowing that his highly personal information, such as his financial information and Social Security number, is no longer confidential and can be used for extortion, theft or fraud, and any number of additional harms against him for the rest of his life.

48. Because AT&T continues to store and share Plaintiffs' and Class Members' PII in the regular course of its business, they have a continuing interest in ensuring that the PII is protected and safeguarded from additional authorized access.

Allegations Relating to Plaintiff Christopher Isbell

49. Plaintiff Christopher Isbell lives and resides in Florida and has been a customer of AT&T for his personal account since 2005.

50. In connection with obtaining AT&T's services, Mr. Isbell was required to provide highly sensitive personal information, such as his contact information, date of birth, Social Security number, and so on. AT&T also prompted Mr. Isbell to create login credentials to access his accounts.

51. In the regular course of business, AT&T shared Mr. Isbell's information with several third-party partners whom AT&T was obligated to verify

their data security practices because those third parties stored the information AT&T collected.

52. Mr. Isbell became aware of the Data Breach on April 1, 2024.

53. Once aware, Mr. Isbell used the website "haveibeenpwned.com"[29] to check if his PII had been part of the AT&T Data Breach. The website confirmed that he was a victim of the Data Breach.

54. Mr. Isbell reviewed AT&T's online notice. The online notice recommends that customers take certain actions like resetting account passcodes and monitoring credit reports for activity and to detect errors. Furthermore, the online notice recommends that customers place a "fraud alert" on their credit report to detect any possible misuse of personal information.

55. As a result of the Data Breach, Mr. Isbell has spent time and effort researching the breach and reviewing his financial statements for evidence of unauthorized activity, which he will continue to do indefinitely.

56. Mr. Isbell also suffered emotional distress knowing that his highly personal information, such as his financial information and Social Security number,

[29] Haveibeenpwned.com is a website created by white hat cybersecurity research Troy Hunt. Mr. Hunt collects and analyzes consumer data that has been posted on the Dark Web to help warn individuals of breaches where their information was impacted and exposed.

is no longer confidential and can be used for extortion, theft or fraud, and any number of additional harms against him for the rest of his life.

57. Because AT&T continues to store and share Plaintiffs' and Class Members' PII in the regular course of its business, they have a continuing interest in ensuring that the PII is protected and safeguarded from additional authorized access.

AT&T Failed to Comply with Federal Law and Regulatory Guidance

58. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decisionmaking.[30] The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[31] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they

---

[30] 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).

[31] *Protecting Personal Information: A Guide for Business,* FTC.ORG, https://www.ftc.gov/businessguidance/resources/protecting-personal-information-guide-business (last visited Jan. 17, 2024).

collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[32]

59. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[33]

60. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal

---

[32] *Id.*

[33] *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).

Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[34]

61. AT&T was fully aware of its obligation to implement and use reasonable measures to protect customers' PII but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. AT&T's failure to employ reasonable measures to protect against unauthorized access to customer information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. Though limited detail is available on the Data Breach, how it occurred or the entity the information originated from, AT&T's failure to safeguard customers' PII suggests AT&T 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, encryption, intrusion detection and prevention, and exercising managerial control over third-party vendors' cybersecurity practices.

The Impact of the Data Breach on Victims'

---

[34] FTC, *Privacy and Security Enforcement,* FTC.GOV, https://www.ftc.gov/news-events/media-resources/protecting-consumerprivacy/privacy-security-enforcement (last visited Jan. 17, 2024).

63. AT&T's failure to keep Plaintiffs' and Class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, date of birth, Social Security numbers, and potentially other sensitive information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class members now and into the indefinite future.

64. As a result, Plaintiffs and Class members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach. Indeed, Plaintiffs' and Class members PII have already been published to the Dark Web available for any cybercriminal to misuse.

65. As discussed above, the PII likely exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[35]

[35] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

66. Further, malicious actors may 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 actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

67. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[36]

68. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;

[36] http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 17, 2024)

- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% report problems with family members as a result of the breach;
- 10% reported feeling suicidal.[37]

69. Identity theft can also exact a physical toll on its victims. A similar survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[38]

---

[37] 2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Jan. 17, 2024).

[38] *Identity Theft: The Aftermath 2017,* https://www.idtheftcenter.org/wp-

70. The unauthorized disclosure of the sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[39]

71. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense. And here, Plaintiffs' and Class members PII is already available to criminal actors on the dark web.

72. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

---

content/uploads/images/pagedocs/Aftermath_2017.pdf (last visited Jan. 17, 2024).

[39] *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.").

73. the unconsented disclosure of confidential information to a third party;

74. losing the value of the explicit and implicit promises of data security;

75. identity theft and fraud resulting from the theft of their PII;

76. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

77. anxiety, emotional distress, and loss of privacy;

78. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

79. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

80. lowered credit scores resulting from credit inquiries following fraudulent activities;

81. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised

accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

82. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

83. Plaintiffs and Class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[40]

84. Because of the value consumers place on data privacy and security, telecommunication businesses with robust data security practices are viewed more favorably by consumers and can command higher prices than those who do not. Consequently, had customers known the truth about AT&T's data security practices—that it did not adequately protect and store PII or adequately monitor the

[40] https://www.fireeye.com/blog/executive-erspective/2016/05/beyond_the_bottomli.html (last visited Jan. 17, 2024).

data security of third-party partners—they would not have contracted with AT&T or would have paid significantly less. As such, Plaintiffs and Class members did not receive the benefit of their bargain with AT&T because they paid for the value of services they did not receive.

85. Plaintiffs 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. Because AT&T failed to live up to its promises and duties in this respect, Plaintiffs and Class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by AT&T's wrongful conduct. Through this remedy, Plaintiffs and Class members seek to restore themselves and class members as close to the same position as they would have occupied but for AT&T's wrongful conduct, namely their failure to adequately protect Plaintiffs' and Class members' PII.

86. Plaintiffs and Class members further seek to recover the value of the unauthorized access to their PII permitted through AT&T's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable

use value of the IP—*i.e.,* a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non- practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions.

87. AT&T's delay in disclosing the Data Breach and notifying victims also caused Plaintiffs and Class members harm. For example, the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. Despite the Data Breach occurring in 2021, AT&T still has not explained the precise nature of the attack, the identity of the hackers, or from whom consumers' PII originated. This is because AT&T ignored the 2021 claims that its customers' PII was being auctioned on the dark web. Had AT&T took the 2021 cybersecurity incident seriously and promptly conducted an adequate investigation, Plaintiffs' and Class members' PII likely would not have been exposed almost three years later. AT&T's decision to forgo an adequate investigation to

discover these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting years to acknowledge, verify, and disclose the Data Breach, AT&T prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

88. Because AT&T continue to hold the PII of customers, Plaintiffs and Class members have an interest in ensuring that their PII is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

89. Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring this action on behalf of themselves and the Class defined as: All individuals whose personal information was compromised in the Data Breach announced by AT&T in March 2024 (the "Class").

90. Specifically excluded from the Class are AT&T; its officers, directors, or employees; any entity in which AT&T has a controlling interest; and any affiliate, legal representative, heir, or assign 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.

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

92. 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 in the Data Breach.

93. Typicality: Plaintiffs' 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.

94. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and his interests are aligned with Class members' interests. Plaintiffs were subject to the same Data Breach as class members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

95. 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. These common questions predominate over any questions affecting only

individual class members. The common questions of law and fact include, without limitation:

- Whether AT&T owed Plaintiffs and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;
- Whether AT&T owed Plaintiffs and Class members a duty to exercise due care in partnering with its third-party vendors who it shares PII and conducting oversight over third-party vendors to ensure they maintained adequate data security to protect Plaintiffs' and Class Members' PII in the course of carrying out the business of their partnership;
- Whether AT&T received a benefit without proper restitution making it unjust for AT&T to retain the benefit without commensurate compensation;
- Whether AT&T acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;
- Whether AT&T violated its duty to exercise due care in partnering with third-party vendors who its shares PII and conducting oversight over these third-party vendors to ensure they maintained adequate data security to protect Plaintiffs' and Class Members' PII in the course of carry out the business of the partnership;

- Whether AT&T breach of its duty to exercise due care and conduct oversight over third-party vendors' data security practices directly and/or proximately caused damages to Plaintiffs and Class members;
- Whether AT&T violated its duty to implement reasonable security systems to protect Plaintiffs' and Class members' PII;
- Whether AT&T breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class members;
- Whether AT&T adequately addressed and fixed the vulnerabilities that enabled the Data Breach;
- Whether Plaintiffs and Class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of personal information;
- Whether AT&T provided timely notice of the Data Breach to Plaintiffs 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.

96. AT&T has engaged in a common course of conduct and Plaintiffs and Class members have been similarly impacted by its failure to maintain reasonable security procedures and practices to protect consumers' PII, as well as AT&T's failure to timely alert affected customers to the Data Breach.

97. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

98. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

99. Defendant AT&T required Plaintiffs' and Class members' PII as a condition to receiving AT&T's services. AT&T collected and stored this PII for commercial gain. AT&T collected, stored, and through the its partnership with third-party vendors, shared the data with these vendors for providing AT&T's services as well as commercial gain.

100. AT&T owed Plaintiffs and Class members, upon partnering with its vendors, a duty to supervise and ensure its vendors maintained adequate data security for the protection of Plaintiffs' and Class members' PII within its control for the purpose of carrying out the business of the partnership consistent with industry standards. AT&T owed a duty to exercise reasonable care in protecting Plaintiffs' and Class members' PII from unauthorized disclosure or access. AT&T acknowledged this duty in its privacy policies describing its handling of PII, where they promised not to disclose PII without authorization.

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

102. AT&T owed a duty of care to Plaintiffs and Class members to remedy any flaws within their system without undue delay so as to alleviate the risk of compromising Plaintiffs' and Class members' PII.

103. AT&T duty to use reasonable care in protecting PII arises because of the parties' relationship, as well as common law and federal law, including the FTC regulations described above and AT&T's own policies and promises regarding privacy and data security.

104. AT&T knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location for the purpose of carrying out the business

of the partnership, its vendors' vulnerability to network attacks, and the importance of adequate security.

105. AT&T breached its duty to Plaintiffs and class members in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class members;
- Failing to ensure its vendors implemented adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class members;
- Failing to supervise its vendors regarding vendors' data security systems, protocols, and practices when it knew or should have known those systems, protocols, and practices were inadequate;
- Failing to comply with industry standard data security measures for the telecommunications industry leading up to the Data Breach;
- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;
- Failing to adequately monitor, evaluate, and ensure the security of their vendors' network and systems;

- Failing to recognize in a timely manner that PII had been compromised; and
- Failing to timely and adequately disclose the Data Breach.

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

107. AT&T's failure to take proper security measures to protect the sensitive PII of Plaintiffs 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, Plaintiffs 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.

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

109. As a direct and proximate result of AT&T's conduct, Plaintiffs and Class members have and will suffer damages including: (i) the loss of rental or 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.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

110. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

111. 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).

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

113. 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 Plaintiffs 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.

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

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

116. 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 Plaintiffs and Class members. As a direct and proximate

result of AT&T's negligence *per se,* Plaintiffs and Class members sustained actual losses and damages as alleged herein. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT III
Breach of Contract
(On Behalf of Plaintiffs and the Class)

117. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

118. 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 Plaintiffs and Class members.

119. Plaintiffs 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.

120. AT&T promised in its Privacy Notice that it would AT&T claims 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."

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

122. As a direct and proximate result of these breaches, Plaintiffs 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. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

123. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs and asserts this claim in the alternative to his breach of contract claim to the extent necessary.

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

125. As part of these transactions, AT&T agreed to safeguard and protect the PII of Plaintiffs 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.

126. 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 Plaintiffs and Class members from unauthorized disclosure or access.

127. Plaintiffs 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. Plaintiffs 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.

128. Plaintiffs 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 Plaintiffs' and Class members' PII was critical to realizing the intent of the parties.

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

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

131. As a direct and proximate result of AT&T's breaches, Plaintiffs 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. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

132. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

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

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

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

136. The price for wireless services that Plaintiffs 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.

137. Likewise, in exchange for receiving Plaintiffs' 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.

138. As a result of AT&T's conduct, Plaintiffs 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 Plaintiffs and Class members all unlawful or inequitable proceeds they received from Plaintiffs and Class members, including damages equaling the difference in value between cable services that included implementation of reasonable data privacy and security practices that Plaintiffs and Class members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT VI
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

139. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

140. 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.

141. 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 Plaintiffs and Class members from further cyberattacks and data breaches that could compromise their PII.

142. AT&T still possesses PII pertaining to Plaintiffs and Class members and continues to share this PII with its vendors, which means Plaintiffs' and Class members' PII remains at risk of further breaches because AT&T's data security measures remain inadequate. Plaintiffs 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.

143. Pursuant to the Declaratory Judgment Act, Plaintiffs 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 (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 Plaintiffs' 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 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, Plaintiffs, on behalf of themselves 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 Plaintiffs as class representatives and Plaintiffs' 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 Plaintiffs and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count 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 their unlawful acts, omissions, and practices;

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

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

Plaintiffs hereby demand a jury trial in the instant action.

[Signature to follow on next page]

Dated: April 2, 2024

Respectfully submitted,

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

Norman E. Siegel*
J. Austin Moore*
Stefon J. David*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
david@stuevesiegel.com

Amy E. Keller*
DICELLO LEVITT LLP
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Tel: 312-214-7900
akeller@dicellolevitt.com

Douglas J. McNamara*
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW, Fifth Floor
Washington, D.C. 20005
Tel. 202-408-4651
dmcnamara@cohenmilstein.com
* *Pro hac vice* applications forthcoming

Attorneys for Plaintiffs and the Proposed Class