

W. Mark Lanier
THE LANIER LAW FIRM, P.C.
10940 W. Sam Houston Pkwy N. Ste. 100
Houston, Texas 77064
Tel: (713) 659-5200
Email: mark.lanier@lanierlawfirm.com

Lead and Liaison Counsel for MDL 3114

[Additional Counsel on Signature Page]

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

IN RE: AT&T INC. CUSTOMER DATA
SECURITY BREACH LITIGATION

This Document Relates to All Cases

§
§ CASE NO. 3:24-cv-00757-E
§
§ MDL DOCKET NO.: 3:24-md-03114-E
§
§ CONSOLIDATED MDL DOCKET
§

MASTER CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
OVERVIEW.....	1
INTRODUCTION	2
JURISDICTION AND VENUE.....	7
PARTIES.....	9
A. Defendants	9
B. Plaintiffs.....	13
FACTUAL BACKGROUND	60
A. AT&T Collects and Stores Its Current and Former Customer’s Personal and Sensitive Information.....	60
B. AT&T Has a History of Mismanaging and Failing to Protect Sensitive and Personal Consumer Information	64
1. AT&T Data Breaches in 2023-2024 Demonstrate Flawed Security Measures and Corporate Mismanagement of Customer Personal Sensitive Information	65
2. AT&T Discloses Its Second Major Breach of Customer Data In 2024....	67
C. AT&T Failed to Protect Former and Current Customers’ Sensitive Personal Information	73
1. AT&T’s Systems Were Compromised by ShinyHunters, and Personal Identifying Information of Over 70 Million Customers Was Exfiltrated and Posted on the Dark Web	73
2. ShinyHunters’ Tactics Are Well Known in the Cybersecurity Industry ..	79
3. AT&T Could Have (and Should Have) Secured Their Systems Against an Attack by ShinyHunters.....	86
4. AT&T Represents that It Has Cybersecurity Expertise, and It Should Have Been Well Equipped to Prevent a Data Breach	90
D. AT&T Had A Duty To Follow Guidance And Industry-Standard Cybersecurity Practices	93

1.	FCC’s Consent Decrees	93
2.	FTC Guidance Regarding Safeguarding Customer Data.....	96
3.	SEC Reporting Requirements	99
4.	Industry Standard Reporting Requirements.....	99
5.	Industry Standards Regarding Network Security	102
E.	The Effect of the AT&T Data Breaches on Plaintiffs and Class Members	106
1.	Plaintiffs’ PII Has Measurable Intrinsic Value	111
2.	Privacy Can Also Be Measure By Cost Paid For It.....	112
	CLASS ALLEGATIONS.....	117
	CHOICE OF LAW	123
	COUNT 1	
	VIOLATION OF THE COMMUNICATIONS ACT.....	125
	COUNT 2	
	VIOLATION OF THE SATELLITE HOME VIEWER EXTENSION AND	
	REAUTHORIZATION ACT.....	129
	COUNT 3	
	VIOLATION OF THE CABLE TELEVISION CONSUMER PROTECTION AND	
	COMPETITION ACT	133
	COUNT 4	
	BREACH OF IMPLIED CONTRACT	138
	COUNT 5	
	NEGLIGENCE	139
	COUNT 6	
	DECLARATORY AND INJUNCTIVE RELIEF	146
	PRAYER FOR RELIEF	147
	JURY TRIAL DEMANDED	148

OVERVIEW

Plaintiffs Anthony Burris, Nella Citino, Jeffery Clark, Brandon Clawson, Michael Crain, Linda Dale, Brittany Ertola, Yajaira De La Espada, Brenda Friend, Bart Gillen, Brittany Hill, Kimberly Holestin, Ashley Jones, Kayla Lee, Charles Leonard, Craig Marsh, Sean Michael McLean, David Meyer, Justin Mitchum, Corrie Mueller, Trevor Nordell, Ja’Vondrick Orange, Tyrone L. Ross, Maria Angelica San Felipe, Azima Sharrieff, Iris Shiver, Paul Taylor, David Vita, and Jessica Wheeler (“**AT&T-Direct Plaintiffs**”), individually and on behalf of the below-defined nationwide classes and nationwide subclasses (“**Classes**,” and Members of the Classes, including Plaintiffs, are referred to as “**Class Members**”) allege the following against Defendants AT&T Inc., AT&T Mobility LLC, AT&T Corporation, and DirecTV, LLC (together, “**AT&T-Direct**” or “**AT&T 1**” or “**AT&T-Direct Defendants**”), based upon personal knowledge, the investigation of counsel, and on information and belief as to all other matters.

Plaintiffs Latosha Austin, Gilbert Criswell, David Hornthal, Traci Lively, Natasha McIntosh, Tim Scaman, and Debby Worley, together with the four AT&T Direct Plaintiffs Yajaira De La Espada, Brenda Friend, Justin Mitchum and Jessica Wheeler (“**AT&T-Snowflake Plaintiffs**”), individually and on behalf of the below-defined AT&T-Snowflake Settlement Class and nationwide subclasses allege the following against Defendants AT&T Inc., AT&T Mobility LLC, AT&T Services, Inc., and Cricket Wireless LLC (and Cricket Wireless LLC (together, “**AT&T-Snowflake**” or “**AT&T 2**” or “**AT&T-Snowflake Defendants**”), based upon personal knowledge, the investigation of counsel, and on information and belief as to all other matters.

Collectively, the AT&T-Direct Plaintiffs and AT&T-Snowflake Plaintiffs shall be referred to as “**Plaintiffs**” and the AT&T-Direct Defendants and AT&T-Snowflake Defendants shall be referred to as “**AT&T**” or “**Defendants.**”

INTRODUCTION

1. AT&T is the world’s third largest telecommunications company. It has over 140,000 employees worldwide and, in 2024, generated over \$122 billion in revenue.¹ As a titan in an industry built on the transmission of extremely sensitive information, AT&T should have had industry-leading security systems in place. It is bound—by both contract and law—to safeguard that information, prevent its misuse or compromise, and promptly notify customers and regulators if a breach occurs. AT&T repeatedly failed at each of its duties.

2. Personally Identifiable Information (“**PII**”)² is immensely valuable, and while it can serve legitimate purposes, it can just as easily be exploited—fueling financial fraud among a range of other harms. In the course of its business operations, AT&T obtained and cultivated the sensitive PII for 7.6 million current AT&T account holders and 65.4 million former AT&T account holders, and promised to keep that information secure and safeguarding their PII from, among other things, being used for illicit purposes. AT&T promised, as it must, that its internal cybersecurity was sufficient to ensure that its treasure trove of PII was protected from unauthorized

¹ AT&T Inc., 2024 Annual Report, (Apr. 4, 2025), available at <https://investors.att.com/~media/Files/A/ATT-IR-V2/financial-reports/annual-reports/2024/complete-annual-report-2024.pdf>.

² The National Institute of Standards and Technology (“NIST”) is an agency of the United States Department of Commerce that promotes American innovation and industrial competitiveness. Pertaining to cybersecurity, the NIST develops standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. One of the most widely cited legal definitions of PII comes from an NIST publication that defines it as “any information about an individual maintained by an [organization], including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.” See Erika McCallister, Tim Grance & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST Special Publication 800-122, NAT’L INST. OF STANDARDS & TECH. (Apr. 2010), <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.

disclosure. AT&T also promised that data would be deleted, as it must, once it no longer served a legitimate business interest in the context upon which it was provided. Yet AT&T failed to secure Plaintiffs' data, failed to timely delete this data for tens of millions of former AT&T customers, and, when the data was breached, failed to promptly notify the millions of current and former customers of that breach so that they could seek to protect themselves.

3. In 2019 ATT's systems were compromised by a third-party threat actor in a data breach ("**AT&T-Direct Data Breach**").³ While the compromised PII varies for each affected customer, at a minimum it comprises variations of email and mailing addresses, full names, phone numbers, Social Security Numbers ("**SSNs**"), dates of birth, AT&T account numbers, and passcodes (collectively referred to as the "**Data Set**").

4. Each AT&T-Direct Plaintiffs' PII is confirmed to have been contained in the Data Set and, thus, compromised in the AT&T-Direct Data Breach. Despite its knowledge of the breach and its knowledge of the harm its customers were exposed to by the breach, AT&T did nothing. By August 20, 2021, the Data Set was known to be published on the Dark Web⁴ by a hacking group colloquially known as ShinyHunters who either bought the Data Set from an unknown threat actor or acquired it through their own exfiltration.⁵

³ Aimee Ortiz, *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, NEW YORK TIMES (Mar. 30, 2024), https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html?unlocked_article_code=1.AE8.ZKnQ.kFry9fYOIkg2&smid=url-share.

⁴ The Dark Web is defined for the purpose of the Complaint as follows: "Many academics and security professionals understand the term '*Dark Web*' generally to describe web services hosted on the Tor Network. These *hidden services* (now called *onion services*) use a so-called onion address to allow users to connect anonymously and also allow the website itself to hide its location and identity from the users, making them very difficult to shut down or censor." See Ben Collier, *Tor: From the Dark Web to the Future of Privacy*, Ch. 7 at 124 (MIT Press 2024).

⁵ Ravie Lakshmanan, *Researchers Detail Modus Operandi of ShinyHunters Cyber Crime Group*, THE HACKER NEWS (Aug. 23, 2021), <https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html>.

5. On March 30, 2024, three years after the first attempted sale (and news reports) were released concerning the Data Set, AT&T finally came clean and announced that the Data Set had been stolen and contained the PII of millions of its current and former customers. Only then, after the Data Set had been circulating on the Dark Web for years, did AT&T notify its customers (current and former) to reset their passcodes. Yet during the years that AT&T refused to acknowledge the AT&T-Direct Data Breach, customer accounts, along with their identities, were vulnerable.

6. The AT&T-Direct Data Breach was the result of *years* of long-standing critical and systemic cybersecurity failures at the company. *First*, AT&T failed to have adequate monitoring and controls in place both internally and for its vendors and therefore failed to detect the breach in 2019. *Second*, and perhaps most importantly, for *years* AT&T failed to conduct a reasonable investigation into the existence or source of the AT&T-Direct Data Breach even after being informed customer data was circulating on the Dark Web.⁶ *Third*, AT&T failed to implement a comprehensive data retention and deletion policy in violation of its Privacy Notice,⁷ a prior Order and Consent Decree by the FCC, and applicable data protection statutes and regulations.⁸

7. AT&T's failure to prevent the AT&T-Direct Data Breach, its lack of investigation, and its five-year delay in disclosing the breach to consumers exemplifies a longstanding pattern of reckless disregard for the privacy and security of consumers' PII. Over the past decade, AT&T has

⁶ *Id.*

⁷ AT&T failed to "destroy [former customer PII] by making it unreadable or indecipherable" as promised in its Privacy Notice. See AT&T Privacy Notice, AT&T, available at <https://about.att.com/privacy/privacy-notice.html> (last visited Apr. 30, 2025).

⁸ See Consent Decree, *In the Matter of AT&T Services, Inc.*, File No.: EB-TCD-14-00016243AT&T (FCC Apr. 8, 2015) ("2015 Consent Decree"), <https://docs.fcc.gov/public/attachments/DA-15-399A1.pdf>.

repeatedly come under scrutiny by federal regulators for its inadequate privacy practices. Both the Federal Communications Commission (“FCC”) and the Federal Trade Commission (“FTC”) have investigated and penalized AT&T for failing to implement reasonable safeguards for customer data.⁹ These enforcement actions have led to multiple fines, formal admonishments, and widespread criticism from lawmakers. The FCC explicitly reprimanded AT&T for “failing to take reasonable steps to protect its customers’ location information.”¹⁰

8. As a result of the AT&T-Direct Data Breach, the AT&T-Direct Plaintiffs have already suffered harm, including: savings fraudulently drained from their accounts;¹¹ unauthorized loans taken out in their name;¹² credit ratings dropping precipitously due to fraudulent activity on their accounts,¹³ and frequent spam calls, texts and emails on the same phone number and email address they provided to AT&T.¹⁴ Many of the AT&T-Direct Plaintiffs spent considerable time—and still spend considerable time—monitoring their accounts. Many also suffered significant out-of-pocket expenses from the exposure of personal data and because of identity theft or fraud.

⁹ *Id.*

¹⁰ *Id.*

¹¹ For example, after the AT&T-Direct Data Breach, Plaintiff Ashley Jones had an unauthorized CareCredit account opened in her name in or about June 2023 with approximately \$12,000 outstanding on the account balance.

¹² For example, Plaintiff Sean Michael McClean had an unauthorized and unknown person apply for a loan in the amount of \$1,000 in his name at a paycheck advance company. Plaintiff subsequently found an unauthorized loan in his name on his credit report.

¹³ For example, Plaintiff Brittany Hill’s credit score plummeted fifty points as a result of fraud she suffered from the AT&T-Direct Data Breach. As a result, it has become more difficult to borrow and use credit.

¹⁴ For example, after the AT&T-Direct Data Breach, Plaintiff Azima Sharrieff received such an incredible amounts of spam calls and texts on the phone number she provided to AT&T that she filed a police report and changed her phone number.

9. While AT&T was still addressing the consequences of the initial data breach, basic lapses in data security practices led to a second data breach, which compromised distinctively sensitive information. On or about July 12, 2024, AT&T announced that data of “nearly all” its cellular customers from May 1, 2022, to October 31, 2022, and January 2, 2023, was illegally downloaded from its workspace on a third-party cloud platform provided by Snowflake, Inc. (the **“AT&T-Snowflake Data Breach”**).

10. In the AT&T-Snowflake Data Breach, call and text records of nearly all of AT&T’s cellular customers, customers of mobile virtual network operators (MVNOs) using AT&T’s wireless network, and AT&T’s landline customers who interacted with those cellular numbers were exposed to unauthorized parties. The records identified telephone numbers with which an AT&T or MVNO wireless number interacted during these periods, counts of interactions, and aggregate call durations. For a subset of records, cell site identification numbers were also included, which can be used to determine approximate locations where calls were made or text messages sent.

11. The AT&T-Snowflake Data Breach was caused by substantially similar security failures as the AT&T-Direct Data Breach, including failure to implement basic multi-factor authentication, failure to rotate credentials, and failure to limit access to trusted locations or users.

12. The compromised information in the AT&T-Snowflake Data Breach is sensitive. With the information, cybercriminals can identify relationships among phone numbers, allowing hackers to make scams more believable.¹⁵

¹⁵ Ramishah Maruf, *How AT&T customers can protect themselves in the latest data breach*, CNN (July 12, 2024), <https://www.cnn.com/2024/07/12/business/att-customers-data-breach-protection/index.html>.

13. As a result of these two Data Breaches, Plaintiffs have already suffered harm, including: savings fraudulently drained from their accounts; unauthorized loans taken out in their name; credit ratings dropping precipitously due to fraudulent activity on their accounts; becoming the target of sophisticated hacking attacks as well as other criminal activity; and frequent spam calls, texts and emails on the same phone number and email address they provided to AT&T. Many Plaintiffs spent considerable time—and still spend considerable time—monitoring their accounts. Many also suffered significant out-of-pocket expenses from the exposure of personal data and because of identity theft or fraud.

14. As a result of the AT&T Data Breaches, in addition to actual harm, including identity theft and fraud, Plaintiffs and Class Members face a substantial risk of imminent and certainly impending harm, heightened here by the loss of the AT&T-Direct Plaintiffs' Social Security numbers – a class of PII which is particularly valuable to identity thieves. Plaintiffs and Class Members have and will continue to suffer injuries associated with this risk, including, but not limited to, a loss of valuable time and opportunity costs and mitigation expenses over the misuse of their PII.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiffs' claims arise under the Communications Act of 1934 ("Communications Act"), 47 U.S.C. § 201, *et seq.*, the Cable Communications Policy Act of 1984 ("Cable Act"), 47 U.S.C. § 551, and the Satellite Home Viewer Extension and Reauthorization Act of 2010 ("Satellite Act"), 47 U.S.C. § 338(i).

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

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

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

18. This Court has personal jurisdiction over AT&T Inc. because AT&T Inc. is headquartered and regularly conducts business in the State of Texas.

19. This Court also has personal jurisdiction over AT&T Mobility, LLC (“AT&T Mobility”) and DirecTV, LLC (“DirecTV”) as at all relevant times they were wholly owned subsidiaries of AT&T Inc. and thus purposefully directed their activities at this forum through conducting business with their corporate parent. Defendants AT&T Mobility and DirecTV also sold, marketed, and advertised their products and services to Plaintiffs Michael Crain, Yajaira De La Espada, Corrie Mueller and Ja’Vondrick Orange, and other similarly situated Class Members, in the State of Texas, and therefore, have sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary. Plaintiffs’ claims arise or relate to those activities, and so jurisdiction comports with traditional notions of fair play and substantial justice.

20. This Court also has personal jurisdiction over AT&T Corporation, AT&T Services, Inc. and Cricket Wireless LLC as at all relevant times they were wholly owned subsidiaries of AT&T Inc. and thus purposefully directed their activities at this forum through conducting business with their corporate parent.

21. Moreover, this Court has personal jurisdiction over Defendants pursuant to 28 U.S.C. §1407, Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation, and the June 5, 2024, Transfer Order of the Judicial Panel on Multidistrict

Litigation (“JPML”) in MDL 3114 (“Transfer Order”) related to this matter, and any future Transfer Orders as the JPML may enter.

22. Venue is proper in this District under 28 U.S.C. §1407, Rule 7.1 of the Rules of Procedure of the JPML, and the Transfer Order related to this matter and any future Transfer Orders as the JPML may issue. In the alternative, venue is proper in this District pursuant to 28 U.S.C. § 1391, because AT&T’s principal place of business is in this District.

PARTIES

A. DEFENDANTS

AT&T Inc.

23. Defendant AT&T Inc. is a Delaware corporation, with its headquarters and principal place of business located at 208 South Akard Street, Dallas, Texas.

24. Defendant AT&T Corporation is a subsidiary of Defendant AT&T Inc.

25. AT&T Inc. is one of the largest wireless carrier in the United States, with over 100 million current subscribers, and earning \$122.43 billion in revenue in 2023 and \$122.06 billion in 2024.

26. On March 5, 2006, AT&T Inc. announced its acquisition of BellSouth Corporation, which consolidated ownership of Cingular Wireless. Cingular Wireless customers became AT&T customers, and AT&T Inc. became the custodian of their PII.

27. On June 29, 2007, AT&T Inc. announced its acquisition of Cellular One, adding approximately 2 million subscribers. Cellular One customers became AT&T customers, and AT&T Inc. became the custodian of their PII.

28. In 2013 and 2014, AT&T Inc. bought Leap Wireless, also known as Cricket, to give customers more access to mobile internet services. Cricket customers became AT&T customers, and AT&T Inc. became the custodian of their PII.

29. On May 18, 2014, AT&T Inc. announced its acquisition of DirecTV, making it the world's largest pay TV provider. In September 2024, AT&T Inc. announced that it was selling its majority stake in DirecTV to a private equity firm as it winds down its entertainment business. But at the time of the AT&T-Direct Data Breach, DirecTV was an AT&T Inc. subsidiary and, on information and belief, was impacted by the unlawful disclosure of customer information in the Data Breach.

30. On June 14, 2018, AT&T Inc. completed the acquisition of Time Warner, which was renamed WarnerMedia. AT&T Inc. notably justified this merger in response to antitrust litigation by emphasizing the value of its customers' data: as part of a vertically integrated entity, WarnerMedia could use the information AT&T Inc. derived about its customers' viewing habits from its DirecTV, U-Verse, and mobile networks to identify what advertisements would be most interesting to those customers, thus justifying higher prices for those ads. *See U.S. v. AT&T Inc.*, 310 F.Supp.3d 161, 177-79, 182-83 (D.D.C. 2018) ("AT&T will also, with their customers' permission, use consumer data to develop targeted ads, thereby increasing the value of Time Warner's ad inventory."); *see also U.S. v. AT&T Inc.*, 916 F.3d 1029, 1033-35 (D.C. Cir. 2019).

31. Once the merger was approved, AT&T Inc. then reorganized its operations into a *Communications* segment (encompassing AT&T Mobility, DirecTV, and U-Verse service), *WarnerMedia* (encompassing Turner television networks, HBO, and Warner Bros. properties), and an *Advertising* segment. While AT&T Inc. later spun off WarnerMedia and merged it with Discovery to form Warner Brothers Discovery in 2022, this corporate structure was in place at the

time of the Data Breach in 2019; based on AT&T Inc.'s representations in the antitrust litigation, its customers' data would have been shared across all of these segments, thus imposing concomitant duties to secure and safely handle that information

32. In short, AT&T Inc. has engaged in many mergers, acquisitions, and restructurings of its telecommunications business and, over the years, has purchased additional entities that later became affiliates and subsidiaries of the AT&T brand of companies. AT&T Inc. has also taken and maintains custody and control of these customers' data.

33. As the corporate parent, AT&T Inc. has "centralized many of its business administration and support functions."¹⁶ To that end, AT&T Inc. "shares information within [its] own AT&T companies and affiliates."¹⁷ AT&T Inc. represents to its customers that these companies and affiliates "are bound to process personal data only in accordance with AT&T's instructions and in compliance with applicable data protection laws[.]"¹⁸

34. AT&T Inc. was bound to act in accordance with any applicable law, regulation, and/or standard of care applicable to the management, retention, or disclosure of data for the customers of its affiliates and/or subsidiaries. For example, in handling the data for a subscriber-Verse or DirecTV subscriber, AT&T Inc. was required to act, or cause its subsidiaries to act, in accordance with the Cable Act, 47 U.S.C. § 551, and the Satellite Act, 47 U.S.C. § 338(i), concerning the protection of subscriber privacy. Likewise, concerning the handling of wireless and wired customer data, AT&T Inc. was required to act, or cause its subsidiaries to act, in accordance

¹⁶ Affiliates, AT&T, https://about.att.com/privacy/global_approach/affiliates-mow.html (last visited Apr. 28, 2025).

¹⁷ AT&T Privacy Notice, AT&T, <https://about.att.com/privacy/privacy-notice.html> (last visited Apr. 28, 2025).

¹⁸ Affiliates, *supra* note 21.

with the Communications Act, 47 U.S.C. §§ 201(b), 222(s), concerning the disclosure of customer information. These legal obligations apply throughout the AT&T corporate structure, as compliance with these statutes cannot be circumvented by sharing customer data with a corporate parent. Moreover, as represented by AT&T Inc., its affiliates and subsidiaries “are bound to process personal data only in accordance with AT&T’s instructions[,]” and thus AT&T Inc. is ultimately responsible for ensuring their and its compliance with governing regulatory frameworks.

AT&T Mobility LLC

35. Defendant AT&T Mobility LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia. AT&T Mobility, also known as AT&T Services and marketed as AT&T, is an American telecommunications company. It is a wholly owned subsidiary of AT&T, Inc. and provides wireless services in the United States. AT&T Mobility is one of the largest wireless carrier in the United States, with 114.5 million subscribers as of March 31, 2024.¹⁹

36. Defendant AT&T Services was, for practical purposes, the predecessor to AT&T Mobility and was part of AT&T Corporation.

DirecTV, LLC

37. Defendant DirecTV, LLC is a Delaware limited liability company with its principal place of business in El Segundo, California. DirecTV is a satellite television provider that offers digital and linear television services. On July 24, 2015, after receiving approval from the FCC and the Department of Justice, AT&T acquired DirecTV. At the end of Q1 2021, AT&T disclosed

¹⁹ 1Q2024 Earnings, *Financial and Operational Trends*, AT&T (Apr. 24, 2024), https://investors.att.com/~media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2024/1Q24/T_1Q24_Trending_Schedule.pdf.

that it had 15.9 million pay TV customers, including DirecTV, U-Verse, and DirecTV Stream subscribers. On February 25, 2021, AT&T announced that it would spin-off DirecTV, U-Verse TV, and DirecTV Stream into a separate entity. On September 30, 2024, AT&T announced that they would sell their remaining 70% stake to TPG Inc., a private equity group, for \$7.6 billion. Once the transaction is completed, TPG Inc. will have 100% ownership of DirecTV, splitting the company off from AT&T for the first time since 2015. AT&T and TPG Inc. expect the sale to close in the second half of 2025. Thus, at the time of the Data Breach, DirecTV was a subsidiary of AT&T, Inc.

Cricket Wireless, LLC

38. Defendant Cricket Wireless LLC is a Delaware limited liability company with its principal place of business in Atlanta, Georgia. Cricket Wireless is a wholly owned subsidiary of AT&T Inc. that provides prepaid wireless service. Cricket Wireless uses AT&T's network to provide its services, and Cricket customers were impacted by the AT&T-Snowflake Data Breach.

B. PLAINTIFFS

39. Plaintiffs are individuals who had their PII compromised in the AT&T-Direct Data Breach and/or the AT&T-Snowflake Data Breach and whose information is confirmed to be in the Data Set available on the Dark Web. Plaintiffs bring this action on behalf of themselves and all those similarly situated both across the United States and within their states of residence.

1. AT&T-Direct Plaintiffs

40. AT&T-Direct Plaintiffs purchased and used AT&T products and/or services, as specifically identified in their individual paragraphs below. In connection with their purchases and use of AT&T products and services, AT&T-Direct Plaintiffs provided confidential and sensitive PII to AT&T, as requested and required by AT&T for the provision of its services. AT&T obtained

and continues to maintain AT&T-Direct Plaintiffs' PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

41. AT&T-Direct Plaintiffs entrusted their unique, sensitive PII to AT&T with the understanding that AT&T would keep their information secure and employ reasonable and adequate security measures to ensure their information would not be compromised. AT&T-Direct Plaintiffs relied on AT&T's policies and promises to implement sufficient measures to protect their PII and privacy rights. Had AT&T-Direct Plaintiffs known of AT&T's lax security practices with respect to Plaintiffs' PII, they would not have done business with AT&T; would not have applied for AT&T's services or purchased its products; would not have opened, used, or continued to use AT&T's cell phone and other telecommunications-related services at the applicable rates and on the applicable terms; and/or would have paid less because of the diminished value of AT&T's services.

42. AT&T-Direct Plaintiffs received a data breach notification from AT&T via email, mail, or account notification in March or April 2024, notifying them that their PII was compromised in the AT&T Direct Data Breach.

43. Because only AT&T (and the cybercriminals) have knowledge of precisely what data points were compromised for each individual Plaintiff, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

44. Since learning of the AT&T-Direct Data Breach, the AT&T-Direct Plaintiffs have experienced—and continue to experience—emotional distress, worry, and the well-founded fear that additional, sufficiently imminent harm in the form of identity theft or fraud will occur in the future because their confidential and sensitive PII is now in the hands of criminals and has been

leaked on the Dark Web and, worse, later advertised and made available on the ShinyHunter's open website accessible via Google and other public search engines.

45. Because of the AT&T-Direct Data Breach, the AT&T-Direct Plaintiffs have taken precautions to mitigate the risk of future harm by spending more time checking their credit and financial accounts for any unauthorized activity; obtaining and reviewing credit bureau reports; and purchasing and/or continuing credit monitoring services. Plaintiffs will have to continue these practices indefinitely to protect against fraud and identity theft.

46. AT&T-Direct Plaintiffs place significant value in the security of their PII. The AT&T-Direct Plaintiffs value their privacy and are very concerned about identity theft and the consequences of such theft and fraud resulting from the AT&T-Direct Data Breach. Indeed, the type of PII that was compromised in the AT&T-Direct Data Breach (*i.e.*, name, address, date of birth, social security number) provides cybercriminals with the information necessary for cybercriminals perpetuate the fraud and identity theft experienced by some AT&T-Direct Plaintiffs, as detailed below.

47. Notwithstanding the actual instances of fraud and identity theft experienced by AT&T-Direct Plaintiffs, given the highly sensitive nature of the information stolen and its subsequent exfiltration by unauthorized parties, Plaintiffs have already suffered injury and remain at a substantial and imminent risk of future harm. As a result of the AT&T-Direct Data Breach, the AT&T-Direct Plaintiffs anticipate spending considerable additional time and money on an ongoing basis to mitigate and address the harms caused by the AT&T-Direct Data Breach.

48. Plaintiffs Anthony Burris, Nella Citino, Jeffery Clark, Brandon Clawson, Michael Crain, Linda Dale, Brittany Ertola, Yajaira De La Espada, Brenda Friend, Bart Gillen, Brittany Hill, Kimberly Holestin, Ashley Jones, Kayla Lee, Charles Leonard, Craig Marsh, Sean Michael

McLean, David Meyer, Justin Mitchum, Corrie Mueller, Trevor Nordell, Ja’Vondrick Orange, Tyrone L. Ross, Maria Angelica San Felipe, Azima Sharrieff, Iris Shiver, Paul Taylor, Jessica Wheeler, and David Vita are the AT&T-Direct Plaintiffs.

2. AT&T-Snowflake Plaintiffs

49. AT&T-Snowflake Plaintiffs were customers of AT&T-Snowflake Defendants, or mobile virtual network operators (MVNOs) using AT&T's network during the period of May 1, 2022 to October 31, 2022, and/or January 2, 2023. AT&T-Snowflake Plaintiffs purchased and used telecommunications services from these entities. In connection with their purchases and use of these services, AT&T-Snowflake Plaintiffs provided AT&T confidential and sensitive PII, as requested and required for the provision of these services. In addition, in connection with their use of these telecommunication services, AT&T collected and stored their call and text records and, for some, cell site identification numbers. AT&T obtained and continues to maintain AT&T-Snowflake Plaintiffs’ PII, call and text records, and cell site identification numbers, and has a legal duty and obligation to protect that information from unauthorized access and disclosure.

50. AT&T-Snowflake Plaintiff accountholders received a data breach notification in July 2024 or thereafter, notifying them that their call and text records were compromised in the AT&T-Snowflake Data Breach.

51. Since learning of the AT&T-Snowflake Data Breach, AT&T-Snowflake Plaintiffs have experienced—and continue to experience—identify theft, fraud, emotional distress, worry, intimidation, scams, harassment and compromised physical security stemming from the exposure of their communication patterns and, for some, location information.

52. Because of the AT&T-Snowflake Data Breach, AT&T-Snowflake Plaintiffs have taken precautions to mitigate the risk of future harm by changing their phone numbers, spending

time monitoring their accounts for suspicious activity, obtaining and reviewing credit bureau reports, purchasing and/or continuing credit monitoring service, exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records, and taking other reasonable steps to protect themselves. AT&T-Snowflake Plaintiffs will need to continue these practices indefinitely.

53. AT&T-Snowflake Plaintiffs place significant value in the privacy of their call and text records and location information. The AT&T-Snowflake Plaintiffs value their privacy and are very concerned about the sensitivity of the information taken since it reveals personal connections, relationships, and movements that AT&T-Snowflake Plaintiffs reasonably expected to remain private. In addition, the AT&T-Snowflake Plaintiffs are also very concerned about identity theft, and its severe downstream consequences, since the information taken can be used to, among other things, perpetrate sophisticated and personalized scams.

54. Given the sensitive nature of the information stolen and its subsequent exfiltration by unauthorized parties, AT&T-Snowflake Plaintiffs have already suffered injury and remain at a substantial and imminent risk of future harm.

55. Plaintiffs Latosha Austin, Gilbert Criswell, David Hornthal, Traci Lively, Natasha McIntosh, Tim Scaman, and Debby Worley are the AT&T-Snowflake Plaintiffs.

56. Plaintiffs Yajaira De La Espada, Brenda Friend, Justin Mitchum, and Jessica Wheeler are also AT&T-Snowflake Plaintiffs, as well as AT&T-Direct Plaintiffs.

Alabama

Natasha McIntosh

57. AT&T-Snowflake Plaintiff Natasha McIntosh is a resident of the State of Alabama. Plaintiff McIntosh was a customer of Boost Mobile from 2002 to 2022 and was an employee of

Boost Mobile for a year, starting around 2003. As a condition of receiving telecommunication services from Boost Mobile, she provided Boost Mobile with multiple types of PII at least her name, SSN, email, and payment card information. In connection with her use of these telecommunication services, Boost Mobile and AT&T collected and stored her call and text records and cell site identification numbers. Plaintiff McIntosh's call and text records were compromised in the AT&T-Snowflake Data Breach. Plaintiff McIntosh has been informed that her personal information was found on the dark web. After the Data Breach began, in the spring of 2024, Plaintiff McIntosh received a notice that an unauthorized party had opened an account with a furniture store using her name and phone number. She started to receive calls and texts about repossessions of furniture that she never bought. Since the AT&T-Snowflake Data Breach, Plaintiff McIntosh has experienced an increase in spam and receives approximately 50 spam calls or messages a day. Plaintiff McIntosh has spent countless hours investigating and mitigating against the substantial risks presented by the theft of her PII and sensitive information. These mitigation efforts have included freezing her credit with credit agencies, registering for credit monitoring services, monitoring her credit accounts and reports, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff McIntosh places significant value in the security of her PII and privacy of her call and text records and location information. This information reveals personal connections, relationships, and movements that AT&T-Snowflake Plaintiff McIntosh reasonably expected to remain private. Plaintiff McIntosh entrusted this information to Boost Mobile and AT&T with the understanding that they would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature

of the information stolen, Plaintiff McIntosh has already suffered injury and remains at a substantial and imminent risk of future harm.

California

Latosha Austin

58. Plaintiff Latosha Austin is a resident of the State of California. Plaintiff Austin is a current customer of AT&T and has been a customer since approximately 2000. Plaintiff Austin was also a customer of Cricket Wireless in or around 1999 to 2000. As a condition of receiving services from AT&T, Plaintiff Austin provided AT&T with multiple types of PII. In connection with her use of these telecommunication services, AT&T collected and stored her call and text records and cell site identification numbers. Plaintiff Austin's PII was compromised in the AT&T-Snowflake Data Breach. In October 2024, Plaintiff Austin received a phone call from a number she recognized as formerly belonging to her father, who had recently changed his number due to a surge of spam and phishing calls. The caller left a voicemail requesting money; however, her father did not place the call or leave the voicemail. In April, September, and November 2024, Plaintiff Austin was notified that her PII had been located on the dark web. Since the Data Breach, Plaintiff Austin has experienced a sharp increase in spam communications and now receives approximately one to two spam text messages daily. As a result of the AT&T-Snowflake Data Breach, Plaintiff Austin has spent numerous hours investigating and attempting to mitigate the substantial risks arising from the theft of her sensitive information. These mitigation efforts have included freezing her credit with all major credit bureaus, monitoring her financial accounts and credit reports, researching the breach to understand the scope of her exposure, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Austin places significant value on the privacy and

security of her PII and call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff Austin reasonably expected to remain private. Plaintiff Austin entrusted this information to AT&T with the understanding that AT&T would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, Plaintiff Austin has already suffered injury and remains at a substantial and imminent risk of future harm.

Gilbert Criswell

59. Plaintiff Gilbert Criswell is a resident of the State of California. Plaintiff Criswell is a current customer of AT&T and has used its services for approximately ten years. As a condition of receiving services from AT&T, Plaintiff Criswell provided AT&T with multiple types of PII. Plaintiff Criswell was notified by AT&T that his PII was compromised in the AT&T-Snowflake Data Breach. In connection with his use of these telecommunication services, Boost Mobile and AT&T collected and stored his call and text records and cell site identification numbers. In or around September 2024, Plaintiff Criswell received a security alert from Google notifying him that his account credentials and password had been compromised through the AT&T-Snowflake Data Breach, prompting him to immediately change his password. In December 2024, Plaintiff Criswell received a phone call from a number he recognized and trusted; however, Plaintiff Criswell's AT&T security application, Active Armor, notified him that the call originated from Russia. Plaintiff Criswell did not engage with the caller and marked the number as spam. Around that same time, Active Armor also alerted Plaintiff Criswell to a malicious malware attack on his device, prompting him to reset his mobile phone and back up all data. Also in December 2024, Plaintiff Criswell was informed by Google Security that his PII was located on the dark web. Following the AT&T-Snowflake Data Breach, Plaintiff Criswell experienced a dramatic increase in unsolicited

communications, receiving approximately 50 phishing emails and spam text messages per day. As a result of the AT&T-Snowflake Data Breach, Plaintiff Criswell has spent approximately 4–5 hours per week investigating and mitigating against the ongoing risks associated with the theft of his PII and sensitive information. These mitigation efforts have included blocking spam calls, monitoring for phishing attempts, changing account passwords, freezing his credit with the major credit bureaus, monitoring his credit accounts and reports for fraudulent activity, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Criswell places significant value in the security of his PII and privacy of his call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff Criswell reasonably expected to remain private. Plaintiff Criswell entrusted this information to AT&T with the understanding that they would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, Plaintiff Criswell has already suffered injury and remains at a substantial and imminent risk of future harm.

Brittany Ertola

60. Plaintiff Brittany Ertola is a resident of the State of California and is a former customer of AT&T's DirecTV, U-Verse, Landline, and Home Internet services. As a condition of receiving services from AT&T, Plaintiff Ertola provided AT&T with multiple types of PII. Plaintiff Ertola was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Ertola confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Ertola had several unauthorized fraudulent charges on the

same bank account that was associated with her AT&T services. Plaintiff Ertola also received a letter indicating an unknown and unauthorized person attempted to take out a \$17,000.00 loan in her name. Similarly, Plaintiff Ertola has been signed up for several websites and rewards programs that she did not initiate or authorize. Also, after the AT&T-Direct Data Breach, Plaintiff Ertola received notice that her PII was found on the Dark Web. Additionally, Plaintiff Ertola received and continues to receive incredible amounts of spam calls and texts on the same phone number she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Ertola spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including having her bank cancel and reissue several of her debit cards, changing her passwords, initiating two-factor authentication for her accounts, contacting creditors through Experian to dispute unauthorized activity on her credit report, changing payment settings with her service providers, freezing her credit, initiating fraud alerts for her accounts, and subscribing to Experian for \$28 per month. Plaintiff Ertola places significant value in the security of her PII. Plaintiff Ertola entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Ertola has already suffered injury and remains at a substantial and imminent risk of future harm.

Bart Gillen

61. Plaintiff Bart Gillen is a resident of the State of California and is a former customer of AT&T's DirecTV and Home Internet services. Plaintiff Gillen is a current customer of AT&T's Wireless and Landline services. Plaintiff Gillen is a current customer of HBO Max and was a former customer of HBO through DirecTV. As a condition of receiving services from AT&T,

Plaintiff Gillen provided AT&T with multiple types of PII. Plaintiff Gillen was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Gillen confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Gillen received notice that his PII was found on the Dark Web. Additionally, Plaintiff Gillen received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. Plaintiff Gillen specifically receives phishing emails seeking his credit card information on the same email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Gillen spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including changing his passwords, initiating two-factor authentication for his financial accounts, freezing his credit, monitoring his credit, initiating fraud alerts for his accounts, and continuing his \$9.99 per month Identity Guard subscription. Plaintiff Gillen places significant value in the security of his PII. Plaintiff Gillen entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gillen has already suffered injury and remains at a substantial and imminent risk of future harm.

Maria Angelica San Felipe

62. Plaintiff Maria Angelica San Felipe is a resident of the State of California and is a former customer of AT&T's Home Internet service. As a condition of receiving services from AT&T, Plaintiff San Felipe provided AT&T with multiple types of PII. Plaintiff San Felipe was

notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff San Felipe confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, on or about October 4, 2023, an unknown person fraudulently attempted to open accounts in Plaintiff San Felipe’s name at Wells Fargo, Capital One, and American Express. Plaintiff San Felipe had previously paid her AT&T bill with her Wells Fargo checking account. Also, after the AT&T-Direct Data Breach, Plaintiff San Felipe received notice that her PII was found on the Dark Web. Additionally, Plaintiff San Felipe received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff San Felipe spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including purchasing a \$40 monthly subscription to Experian, working with Wells Fargo, Capital One, and American Express to resolve the fraudulent accounts, closing her preexisting accounts with Wells Fargo, Capital One, and American Express, changing her passwords, initiating two factor authentication for her accounts, freezing her credit, and initiating fraud alerts for her accounts. Plaintiff San Felipe places significant value in the security of her PII. Plaintiff entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff San Felipe has already suffered injury and remains at a substantial and imminent risk of future harm.

Iris Shiver

63. Plaintiff Iris Shiver is a resident of the State of California and is a former customer of AT&T's DirecTV, Landline, Home Internet, U-Verse, and HBO services. Plaintiff Shiver is a current customer of AT&T's Wireless service. As a condition of receiving services from AT&T, Plaintiff Shiver provided AT&T with multiple types of PII. Plaintiff Shiver was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Shiver confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff was targeted in a scheme to steal funds from the same checking account she set up on AutoPay for her AT&T services. Similarly, Plaintiff Shiver had several unauthorized charges on a credit card she used to pay for her AT&T services. Also, after the AT&T-Direct Data Breach, Plaintiff Shiver received notice that her PII was found on the Dark Web. Additionally, Plaintiff Shiver received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Shiver spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including continuing to monitor her accounts for fraudulent activity on a daily basis, closing her accounts, changing her passwords, initiating two-factor authentication for her accounts, utilizing authentication apps, freezing her credit, initiating fraud alerts for her accounts, and subscribing to Identity Works and ARAG Identity Theft Protection. Plaintiff Shiver places significant value in the security of her PII. Plaintiff entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly

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

Paul Taylor

64. Plaintiff Paul Taylor is a resident of the State of California and is a former customer of AT&T's DirecTV Internet services. Plaintiff Taylor is a current customer of AT&T's Wireless and HBO services. As a condition of receiving services from AT&T, Plaintiff Taylor provided AT&T with multiple types of PII. Plaintiff Taylor was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Taylor confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Taylor has had frequent unauthorized fraudulent charges on the debit card he used to pay for his AT&T services. Plaintiff Taylor has had to cancel and reissue this associated debit card numerous times since 2019 due to fraudulent activity. Plaintiff Taylor's cell phone and Uber accounts were also accessed by unknown and unauthorized individuals. Prior to the AT&T-Direct Data Breach, Plaintiff Taylor had never experienced identity theft or other fraudulent activity on his financial accounts. Additionally, Plaintiff Taylor received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Taylor spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including working with Wells Fargo to cancel and reissue his debit cards several times, changing his passwords repeatedly, and initiating two-factor authentication for his accounts. Plaintiff has incurred late fees as a result of

the repeated fraudulent charges and reissued debit cards. Plaintiff Taylor places significant value in the security of his PII. Plaintiff Taylor entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Taylor has already suffered injury and remains at a substantial and imminent risk of future harm.

David Vita

65. Plaintiff David Vita is a resident of the State of California and is a current customer of AT&T's DirecTV, Wireless, Landline, U-Verse, and Home Internet services. Plaintiff Vita had AT&T's HBO service when it was offered for no charge as part of a promotion. As a condition of receiving services from AT&T, Plaintiff Vita provided AT&T with multiple types of PII. Plaintiff Vita was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Vita confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. Plaintiff Vita pays for his AT&T services using his checking account in conjunction with online bill pay and AT&T's AutoPay. After the AT&T-Direct Data Breach, Plaintiff Vita received notice that his PII was found on the Dark Web. Additionally, Plaintiff Vita received and continues to receive incredible amounts of spam emails on the same email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Vita spent time and effort researching the Data Breach, monitoring his accounts for fraudulent activity, and attempting to freeze his credit. Plaintiff Vita places significant value in the security of his PII. Plaintiff entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate

security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Vita has already suffered injury and remains at a substantial and imminent risk of future harm.

District of Columbia

Traci Lively

66. Plaintiff Traci Lively is a resident of the District of Columbia. Plaintiff Lively has been a customer of Cricket Wireless since approximately 2022. As a condition of receiving telecommunication services from Cricket Wireless, Plaintiff Lively provided Cricket with multiple types of PII. In connection with his use of these telecommunication services, Cricket and AT&T collected and stored his call and text records and cell site identification numbers. Plaintiff Lively was notified by AT&T that his PII was compromised in the AT&T-Snowflake Data Breach. Plaintiff Lively received a notice letter from Cricket Wireless dated July 16, 2024, informing him that his PII had been compromised. In the fall of 2024, Plaintiff Lively was informed that there had been approximately ten inquiries into his credit, which were associated with attempts to open unauthorized accounts and loans in his name. Following the AT&T-Snowflake Data Breach, Plaintiff Lively has spent significant time and effort investigating and mitigating against the serious risks posed by the exposure and theft of his PII and call and text records. These mitigation efforts have included researching the data breach, monitoring his credit reports and financial accounts, addressing attempted unauthorized uses of his stolen PII, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Lively places significant value in the security of his PII and privacy of his call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff Lively reasonably expected to remain private. Plaintiff

Lively entrusted this information to Cricket and AT&T with the understanding that they would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, Plaintiff Lively has already suffered injury and remains at a substantial and imminent risk of future harm.

Florida

Kimberly Holestin

67. Plaintiff Kimberly Holestin is a resident of the State of Florida and is a former customer of AT&T's DirecTV, Wireless, Landline, Home Internet, Prepaid, and HBO services. As a condition of receiving services from AT&T, Plaintiff Holestin provided AT&T with multiple types of PII. Plaintiff Holestin was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Holestin confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Holestin had unauthorized charges on the Wells Fargo checking account that was previously set up on AutoPay for her AT&T services. Despite replacing her debit card several times, Plaintiff Holestin continues experiencing problems with unauthorized activity on her Wells Fargo checking account. Plaintiff Holestin also had several vehicles purchased and registered in her name without her authorization. Also, after the AT&T-Direct Data Breach, Plaintiff Holestin received notice that her PII was found on the Dark Web. Additionally, Plaintiff Holestin received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Holestin spent time and effort researching the AT&T-Direct Data Breach and monitoring her accounts for fraudulent activity, including

asking her bank to refund unauthorized charges and reissue debit cards, changing her passwords, initiating two-factor authentication for her accounts, freezing her credit, initiating fraud alerts for her accounts, and subscribing to Experian credit monitoring and LifeLock identity theft protection for a monthly fee. Plaintiff Holestin places significant value in the security of her PII. Plaintiff Holestin entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Holestin has already suffered injury and remains at a substantial and imminent risk of future harm.

Craig Marsh

68. Plaintiff Craig Marsh is a resident of the State of Florida and is a former customer of AT&T's DirecTV, and U-Verse. Plaintiff Marsh is a current customer of AT&T's Wireless, and Home Internet services. Plaintiff Marsh is a current customer of HBO Max and was a former customer of HBO through U-Verse and a previous provider. As a condition of receiving services from AT&T, Plaintiff Marsh provided AT&T with multiple types of PII. Plaintiff Marsh was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Marsh confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Marsh noticed multiple unauthorized charges on his Wells Fargo account, which was an account associated with his AT&T services. Additionally, Plaintiff Marsh also received text messages and a letter from Chase Bank referencing a new checking account an unknown and unauthorized person attempted to open in his name. Plaintiff Marsh had to contact Chase Bank,

stop the account from being opened, and have a flag placed on his record to prevent additional attempts to open accounts in his name. Finally, Plaintiff Marsh had inquiries on his credit report related to two unauthorized consumer credit card credit inquiries that he did not initiate. Additionally, Plaintiff Marsh received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Marsh spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including changing the debit card associated with his compromised bank account, subscribing to Credit Karma for \$6.99 per month, Equifax for approximately \$12 per month, and Experian intermittently, changing his passwords, initiating two-factor authentication for his accounts, and temporarily freezing his credit. Plaintiff Marsh places significant value in the security of his PII. Plaintiff Marsh entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Marsh has already suffered injury and remains at a substantial and imminent risk of future harm.

Georgia

Anthony Burris

69. Plaintiff Anthony Burris is a resident of the State of Georgia and is a former customer of AT&T's DirecTV service. Plaintiff Burris is a current customer of AT&T's Wireless and Home Internet services. As a condition of receiving services from AT&T, Plaintiff Burris provided AT&T with multiple types of PII. Plaintiff Burris was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Burris confirmed that his PII—including

his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Burris had unauthorized charges on his Navy Federal Credit Union checking account that is the same account he set up on AutoPay for his AT&T services. Also, after the AT&T-Direct Data Breach, Plaintiff Burris received notice that his PII was found on the Dark Web. Additionally, Plaintiff Burris received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Burris spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including working with his bank to reissue debit cards on his compromised account, changing his passwords, initiating two-factor authentication for his accounts, freezing his credit, initiating fraud alerts for his accounts, and maintaining subscriptions to Credit Karma, Identity Guard, and Experian. Plaintiff Burris places significant value in the security of his PII. Plaintiff Burris entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm.

Justin Mitchum

70. Plaintiff Justin Mitchum is a resident of the State of Georgia and is a former customer of AT&T's DirecTV service. Plaintiff Mitchum is a current customer of AT&T's Wireless and Home Internet services. As a condition of receiving services from AT&T, Plaintiff Mitchum provided AT&T with multiple types of PII. In connection with his use of these

telecommunication services, AT&T collected and stored his call and text records and cell site identification numbers. Plaintiff Mitchum was notified by AT&T that his PII was compromised in both the AT&T-Direct and AT&T-Snowflake Data Breaches. Plaintiff Mitchum confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, in or about May 2024, upon information and belief, an unauthorized and unknown individual accessed Plaintiff Mitchum's AT&T account and purchased products and services totaling upwards of \$5,000.00. After spending time working with AT&T disputing those charges, he was ultimately unable to get all the charges refunded and thus incurred out-of-pocket losses. As a result of this fraud, Plaintiff Mitchum closed two bank accounts that were associated with his AT&T services. Plaintiff Mitchum has also noticed a significant drop in his credit score since the AT&T-Direct Data Breach. Additionally, Plaintiff Mitchum received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct and AT&T-Snowflake Data Breaches, Plaintiff Mitchum spent time and effort researching the Data Breaches and monitoring his accounts for fraudulent activity, including closing and opening new bank accounts, changing his passwords, initiating two-factor authentication for his accounts, changing his phone number, updating payment settings with his service providers, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Mitchum places significant value in the security of his PII. Plaintiff entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Plaintiff Mitchum

also places significant value on the privacy and security of his call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff Mitchum reasonably expected to remain private. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Mitchum has already suffered injury and remains at a substantial and imminent risk of future harm.

Illinois

David Hornthal

71. AT&T-Snowflake Plaintiff David Hornthal is a resident of the State of Illinois. Plaintiff Hornthal is and during all times concerned herein was an authorized user on his father's AT&T account. As a condition of receiving telecommunication services from AT&T, his information was provided to AT&T, with multiple types of PII including at least his name, physical address, phone number, and payment card information. In connection with his use of these telecommunication services, AT&T collected and stored his call and text records and cell site identification numbers. After the Data Breach began, AT&T sent a data breach notice via email dated July 15, 2024, to the main contact for Plaintiff Hornthal's AT&T account, his father. The notice email listed Plaintiff Hornthal's phone number among those whose data was accessed in the Data Breach. Plaintiff's call and text records were compromised in the AT&T-Snowflake Data Breach. After the AT&T-Snowflake Data Breach, on or about November 17, 2024, an unauthorized party made a fraudulent charge on the credit card Plaintiff Hornthal used to pay for AT&T's services. Since the AT&T-Snowflake Data Breach, Plaintiff Hornthal has experienced an increase in spam and receives several spam calls or messages a day. Plaintiff Hornthal has spent countless hours investigating and mitigating against the substantial risks presented by the theft of his PII and sensitive information. These mitigation efforts have included investigating the

fraudulent charge, contacting his bank, closing and reopening the affected account, monitoring his credit accounts and reports, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Hornthal specifically spent approximately 2-3 hours resetting automatic billing instructions tied to the affected credit card and addressing fees incurred from failed automatic billing attempts on the closed card. Plaintiff Hornthal places significant value in the security of his PII and privacy of his call and text records and location information. This information reveals personal connections, relationships, and movements that AT&T-Snowflake Plaintiff Hornthal reasonably expected to remain private. Plaintiff entrusted this information to AT&T with the understanding that they would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, Plaintiff Hornthal has already suffered injury and remains at a substantial and imminent risk of future harm.

Tim Scaman

72. AT&T-Snowflake Plaintiff Tim Scaman is a resident of the State of Illinois. Plaintiff Scaman was an authorized user on his fiancé's AT&T account from February 2021 to 2023. As a condition of receiving telecommunication services AT&T, his information was provided to AT&T, with multiple types of PII including at least his name, physical address, phone number, and email address. In connection with his use of these telecommunication services, AT&T collected and stored his call and text records and cell site identification numbers. Plaintiff's call and text records were compromised in the AT&T-Snowflake Data Breach. On July 15th, 2024, the account holder for Plaintiff Scaman's AT&T account received a data breach notice from AT&T. Since the AT&T-Snowflake Data Breach, Plaintiff Scaman has experienced an increase in spam and receives several spam calls or messages a day. Plaintiff Scaman has spent countless hours

investigating and mitigating against the substantial risks presented by the theft of his PII and sensitive information. These mitigation efforts have included monitoring his credit accounts and reports, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Scaman places significant value in the security of his PII and privacy of his call and text records and location information. This information reveals personal connections, relationships, and movements that AT&T-Snowflake Plaintiff Scaman reasonably expected to remain private. Plaintiff entrusted this information to AT&T with the understanding that they would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, Plaintiff Scaman has already suffered injury and remains at a substantial and imminent risk of future harm.

Indiana

Jessica Wheeler

73. Plaintiff Jessica Wheeler is a resident of the State of Indiana and is a former customer of AT&T's DirecTV and Home Internet services. Plaintiff Wheeler is a current customer of AT&T's Wireless services. As a condition of receiving services from AT&T, Plaintiff provided AT&T with multiple types of PII. In connection with her use of these telecommunication services, AT&T collected and stored her call and text records and cell site identification numbers. Plaintiff Wheeler was notified by AT&T that her PII was compromised in both the AT&T-Direct and AT&T-Snowflake Data Breaches. Plaintiff Wheeler confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, in or about December 2023, Plaintiff

Wheeler experienced unauthorized charges of \$400 and \$104 on the same debit card that was set up on AutoPay for her AT&T services. Plaintiff Wheeler set up the replacement debit card on AutoPay with AT&T and experienced unauthorized charges again in July 2024. Plaintiff Wheeler incurred late fees totaling approximately \$60 as a result of missing payments due to her compromised debit card. Further, in or about June 2024, Plaintiff Wheeler received an alert indicating that an unknown and unauthorized individual attempted to open a new credit card account in her name with Credit One. Also, after the AT&T-Direct and AT&T-Snowflake Data Breaches, Plaintiff Wheeler received notice that her PII was found on the Dark Web. Additionally, Plaintiff Wheeler received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct and AT&T-Snowflake Data Breaches, Plaintiff Wheeler spent time and effort researching the Data Breaches and monitoring her accounts for fraudulent activity, including canceling her compromised debit cards and obtaining new debit cards, working with the credit bureaus to remove fraudulent activity from her credit report, changing her passwords, initiating two factor authentication for her accounts, initiating fraud alerts for her accounts, updating payment settings with service providers, subscribing to Identity Works identity theft protection services for \$24.99 per month, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Wheeler places significant value in the security of her PII. Plaintiff Wheeler entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Plaintiff Wheeler also places significant value on the privacy and security of her call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff Wheeler

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

Kansas

Trevor Nordell

74. Plaintiff Trevor Nordell is a resident of the State of Kansas and is a former customer of AT&T's DirecTV and Home Internet services. As a condition of receiving services from AT&T, Plaintiff Nordell provided AT&T with multiple types of PII. Plaintiff Nordell was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Nordell confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Nordell had unauthorized charges post to his credit card account. Plaintiff Nordell also had a prepaid/reloadable Card.com credit card opened in his name that he did not authorize or initiate. Also, after the AT&T-Direct Data Breach, Plaintiff Nordell received notice that his PII was found on the Dark Web. Additionally, Plaintiff Nordell received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Nordell spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including freezing his credit with Experian, TransUnion, and Equifax, closing a credit card and having a new card be issued, contacting various banking institutions, consistently reviewing his credit reports for unauthorized activity, filing police reports, and subscribing to Aura for further credit protection. Plaintiff Nordell places significant value in the security of his PII. Plaintiff

Nordell entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Nordell has already suffered injury and remains at a substantial and imminent risk of future harm.

Louisiana

Ashley Jones

75. Plaintiff Ashley Jones is a resident of the State of Louisiana and is a former customer of AT&T's Home Internet service. As a condition of receiving services from AT&T, Plaintiff Jones provided AT&T with multiple types of PII. Plaintiff Jones was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Jones confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Jones had an unauthorized CareCredit account opened in her name in or about June 2023 with approximately \$12,000 outstanding on the account balance. Plaintiff Jones also had various unauthorized charges post to her Discover credit card and Discover debit card in or about January and February 2024. Also, after the AT&T-Direct Data Breach, Plaintiff Jones received notice that her PII was found on the Dark Web. Additionally, Plaintiff received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Jones spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including freezing her credit, futile efforts working with CareCredit to resolve the unauthorized

account, calling Discover Bank to close affected debit and checking accounts and open new accounts, proactively closing an account with Chase Bank for fear of experiencing additional fraud, contacting the credit bureaus, and continually locking her cards in between purchases. Plaintiff Jones places significant value in the security of her PII. Plaintiff entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Jones has already suffered injury and remains at a substantial and imminent risk of future harm.

Michigan

Brenda Friend

76. Plaintiff Brenda Friend is a resident of the State of Michigan and is a current customer of AT&T's Wireless, Landline, and Home Internet services. Plaintiff Friend is a current customer of HBO Max and was a former customer of HBO through a previous provider. As a condition of receiving services from AT&T, Plaintiff Friend provided AT&T with multiple types of PII. In connection with her use of these telecommunication services, AT&T collected and stored her call and text records and cell site identification numbers. Plaintiff Friend was notified by AT&T that her PII was compromised in both the AT&T-Direct and AT&T-Snowflake Data Breaches. Plaintiff Friend confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Friend experienced unauthorized activity on the same checking account she used to pay her AT&T bill. Specifically, in or about May 2019, Plaintiff

Friend was the victim of three unauthorized charges on her Huntington Bank account totaling over \$2,000. The unauthorized charges resulted in an overdraft fee. Plaintiff Friend suffered additional unauthorized fraudulent activity on the same account in 2023, 2024, and 2025. With each occurrence, Plaintiff Friend had to contact her bank to resolve the fraudulent activity and had to pay \$25 to replace her debit card each time. Also, after the AT&T-Direct and AT&T-Snowflake Data Breaches, Plaintiff Friend received notice that her PII was found on the Dark Web. Additionally, Plaintiff Friend received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. In an effort to combat these calls, texts and emails, Plaintiff Friend subscribed to fraud and spam blocking software for \$4.99 per month. As a result of the AT&T-Direct and AT&T-Snowflake Data Breaches, Plaintiff Friend spent time and effort researching the Data Breaches and monitoring her accounts for fraudulent activity, including working with her bank to close compromised accounts and open new accounts, changing her passwords, initiating two-factor authentication for her financial accounts, resetting payment settings with multiple service providers, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Friend places significant value in the security of her PII. Plaintiff entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Plaintiff Friend also places significant value on the privacy and security of her call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff Friend reasonably expected to remain private. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Friend has already suffered injury and remains at a substantial and imminent risk of future harm.

Brittany Hill

77. Plaintiff Brittany Hill is a resident of the State of Michigan and is a former customer of AT&T's Home Internet and U-Verse service. As a condition of receiving services from AT&T, Plaintiff Hill provided AT&T with multiple types of PII. Plaintiff Hill was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Hill confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, in or about September 2023, unknown and unauthorized persons fraudulently applied for credit cards in Plaintiff Hill's name. These applications resulted in multiple hard credit inquiries made on her credit report and caused Plaintiff Hill's credit score to drop approximately fifty points. Unauthorized charges were also posted to Plaintiff Hill's Cash App card, ranging in amounts from \$1 to \$50. Further, in or about 2022, Plaintiff Hill was informed that an account was opened in her name at Chase Bank with multiple transactions listed to and from an unknown PayPal account. Also, after the AT&T-Direct Data Breach, Plaintiff Hill received notice from Experian that her PII was found on the Dark Web as a result of the AT&T-Direct Data Breach. Additionally, Plaintiff Hill received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Hill spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including subscribing to Experian's monthly credit monitoring program, spending hours working with Chase Bank to close the unauthorized and fraudulent account in her name, changing her passwords, and resolving the fraudulent charges posted on her personal bank account. Plaintiff Hill places significant value in the security of her PII. Plaintiff Hill entrusted her sensitive PII to

AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Hill has already suffered injury and remains at a substantial and imminent risk of future harm.

Nevada

Sean Michael McLean

78. Plaintiff Sean Michael McLean is a resident of the State of Nevada and is a former customer of AT&T's DirecTV, Wireless, U-Verse, and Home Internet services. Plaintiff McLean is a current customer of HBO Max and was a former customer of HBO through DirecTV. As a condition of receiving services from AT&T, Plaintiff McLean provided AT&T with multiple types of PII. Plaintiff McLean was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff McLean confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff McLean had unauthorized fraudulent charges on the Credit One credit card account that was a saved payment method for his AT&T services. One attempted charge was approximately \$400 at Target, and the other was approximately \$300 at Home Depot. Plaintiff McLean also had an unauthorized and unknown person apply for a loan in the amount of \$1,000 in his name at a paycheck advance company. Plaintiff McLean subsequently found an unauthorized loan in his name on his credit report. Plaintiff McLean received notices about bank account and credit card applications that he did not initiate. Also, after the AT&T-Direct Data Breach, Plaintiff McLean received notice that his PII was found on the Dark Web. Additionally, Plaintiff McLean received and continues to receive incredible amounts

of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff McLean spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including closing his compromised Credit One account and opening a new one, refuting the fraudulent activities for the attempted loan and credit card application, removing the unauthorized loan from his credit report, changing his passwords, initiating two factor authentication for his accounts, freezing his credit, initiating fraud alerts for his accounts, and subscribing to Experian credit monitoring, FICO for \$80 per month, and Life Lock for \$100 per year. Plaintiff McLean has also had to pay approximately \$30 to replace his breached credit cards. Plaintiff McLean places significant value in the security of his PII. Plaintiff McLean entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff McLean has already suffered injury and remains at a substantial and imminent risk of future harm.

New Jersey

Tyrone L. Ross

79. Plaintiff Tyrone L. Ross is a resident of the State of New Jersey and is current customer of AT&T's DirecTV services. As a condition of receiving services from AT&T, Plaintiff Ross provided AT&T with multiple types of PII. Plaintiff Ross was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Ross confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Ross

experienced unauthorized Wal-Mart purchases on the same debit card he used to pay for his AT&T services. Similarly, another unauthorized purchase appeared on Plaintiff's credit report. In early 2025, Plaintiff Ross found out that an unauthorized and unknown person applied for a driver's license using his PII. Plaintiff Ross also received a letter from AmeriChoice health insurance referencing an account that he never authorized or initiated. Also, after the AT&T-Direct Data Breach, Plaintiff Ross received notice that his PII was found on the Dark Web. Additionally, Plaintiff Ross received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Ross spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including closing his compromised checking account and opening a new checking account, obtaining a new driver's license, changing his passwords, initiating two-factor authentication for his accounts, and resolving late fees he incurred as a result of having to replace his compromised debit card. Plaintiff Ross places significant value in the security of his PII. Plaintiff Ross entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Ross has already suffered injury and remains at a substantial and imminent risk of future harm.

Debby Worley

80. AT&T-Snowflake Plaintiff Debby Worley is a resident of the State of New Jersey. Plaintiff Worley has been a Boost Mobile customer for approximately two to three years. As a condition of receiving telecommunication services from Boost Mobile, she provided Boost Mobile with multiple types of PII. In connection with her use of these telecommunication services, Boost

Mobile and AT&T collected and stored her call and text records and cell site identification numbers. Plaintiff Worley received a notice letter from Boost Mobile dated November 18, 2024, notifying her that her call and text records were compromised in the AT&T-Snowflake Data Breach. Since the AT&T-Snowflake Data Breach, Plaintiff Worley has experienced—and continues to experience—an increase in spam and scam phone calls probing her for information. Plaintiff Worley has spent at least ten hours investigating and mitigating against the substantial risks presented by the theft of her PII and sensitive information. These mitigation efforts have included freezing her credit with credit agencies, registering for credit monitoring services, monitoring her credit accounts and reports, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff Worley places significant value in the security of her PII and privacy of her call and text records and location information. This information reveals personal connections, relationships, and movements that AT&T-Snowflake Plaintiff Worley reasonably expected to remain private. Plaintiff Worley entrusted this information to Boost Mobile and AT&T with the understanding that they would keep it secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, Plaintiff Worley has already suffered injury and remains at a substantial and imminent risk of future harm.

North Carolina

Linda Dale

81. Plaintiff Linda Dale is a resident of the State of North Carolina and is a former customer of AT&T's Landline, U-Verse, and HBO services. Plaintiff Dale is a current customer of AT&T's Wireless and Home Internet services. As a condition of receiving services from AT&T,

Plaintiff Dale provided AT&T with multiple types of PII. Plaintiff Dale was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Dale confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, in April 2024, Plaintiff Dale experienced unauthorized and fraudulent charges on her credit card. Plaintiff Dale cancelled the compromised credit card, obtained a new credit card, and experienced additional unauthorized and fraudulent activity again in May 2024. Plaintiff Dale cancelled the credit card again, and received a second replacement credit card, but no longer uses the credit card due to fear of fraudulent activity. Also in 2024, Plaintiff Dale received two letters in the mail from LendingClub referencing applications made in her name for personal loans which she never applied for or authorized and were later determined to be fraudulent applications. Additionally, Plaintiff Dale received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Dale spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including working with her credit union to cancel her compromised credit cards twice and open new credit cards, freezing her credit with all three credit bureaus, initiating fraud alerts for her accounts, subscribing to Experian credit monitoring, and subscribing to Aura fraud monitoring services for \$144 per year. Plaintiff Dale places significant value in the security of her PII. Plaintiff Dale entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature

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

Ohio

Nella Citino

82. Plaintiff Nella Citino is a resident of the State of Ohio and is a former customer of AT&T's Landline, and U-Verse services. Plaintiff is a current customer of AT&T's Home Internet services. As a condition of receiving services from AT&T, Plaintiff Citino provided AT&T with multiple types of PII. Plaintiff Citino was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Citino confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, in November 2023, Plaintiff Citino experienced unauthorized charges totaling over \$2,000.00 on her Kohl's credit card. Also, after the AT&T-Direct Data Breach, Plaintiff Citino received notice that her PII was found on the Dark Web. Additionally, Plaintiff Citino received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Citino spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including canceling the compromised Kohl's credit card and opening a new Kohl's credit card, contacting her financial institutions to notify them of the Data Breach, changing her passwords, initiating two-factor authentication for her accounts, freezing her credit with all three credit bureaus, and initiating fraud alerts for her accounts. Plaintiff Citino places significant value in the security of her PII. Plaintiff Citino entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure

and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Citino has already suffered injury and remains at a substantial and imminent risk of future harm.

Jeffery Clark

83. Plaintiff Jeffery Clark is a resident of the State of Ohio and is a former customer of AT&T's DirecTV, U-Verse, and HBO services. Plaintiff Clark is a current customer of AT&T's Wireless and Home Internet services. As a condition of receiving services from AT&T, Plaintiff Clark provided AT&T with multiple types of PII. Plaintiff Clark was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Clark confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Clark noticed unauthorized charges totaling several hundred dollars on the same Chase Bank debit card he set up on AutoPay for his AT&T services. After the unauthorized charges, Plaintiff Clark contacted Chase Bank to report the fraud and request a new card. Plaintiff Clark set up the new card on AutoPay for his AT&T services and once again experienced unauthorized charges on that new card starting in May 2024. Additionally, Plaintiff Clark received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Clark spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including canceling his compromised debit cards and obtaining new debit cards, freezing his credit with all three credit bureaus, changing his passwords, initiating two-factor authentication for his accounts,

and updating payment settings with service providers. Plaintiff incurred late fees and lost discounts associated with the payment settings he had to change. Plaintiff Clark places significant value in the security of his PII. Plaintiff Clark entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Clark has already suffered injury and remains at a substantial and imminent risk of future harm.

Pennsylvania

David Meyer

84. Plaintiff David Meyer is a resident of the Commonwealth of Pennsylvania and is former customer of AT&T's DirecTV, Wireless, and HBO services. As a condition of receiving services from AT&T, Plaintiff Meyer provided AT&T with multiple types of PII. Plaintiff Meyer was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Meyer confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Meyer had multiple unauthorized withdrawals from a checking account that was a saved payment method for his AT&T services. Plaintiff Meyer also had several financial accounts fraudulently opened in his name with multiple banks and financial institutions. Also, after the AT&T-Direct Data Breach, Plaintiff Meyer received notice that his PII was found on the Dark Web. Additionally, Plaintiff Meyer received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Meyer spent significant time and effort

researching the Data Breach and monitoring his accounts for fraudulent activity, including, but not limited to, contacting his bank to report fraud and obtain a new debit card, personally contacting the banks and financial institutions to close the accounts that were fraudulently opened in his name, changing his passwords, initiating two-factor authentication for his accounts, and freezing his credit. Plaintiff Meyer places significant value in the security of his PII. Plaintiff Meyer entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Meyer has already suffered injury and remains at a substantial and imminent risk of future harm.

Tennessee

Brandon Clawson

85. Plaintiff Brandon Clawson is a resident of the State of Tennessee and is a former customer of AT&T's DirecTV, Home Internet, HBO, and U-Verse services. Plaintiff Clawson is a current customer of AT&T's Wireless service. As a condition of receiving services from AT&T, Plaintiff Clawson provided AT&T with multiple types of PII. Plaintiff Clawson was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Clawson confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. Additionally, Plaintiff Clawson received, and continues to receive, excessive amounts of spam calls, emails, and texts on the same phone number and email address he provided to AT&T. After the AT&T-Direct Data Breach, Plaintiff Clawson experienced numerous unauthorized and fraudulent charges on his debit cards,

including purchases for food delivery and motel rooms across the country, as well as two fraudulent withdrawals from his personal checking accounts in the amounts of \$2,000 and \$800. The cards with the unauthorized activity were associated with his AT&T account. As a result of the AT&T-Direct Data Breach, Plaintiff Clawson spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including purchasing a monthly subscription for a spam blocking application and LifeLock identity theft protection, and working with his various service providers when he fell behind on his bills after the unauthorized withdrawals from his personal checking account occurred. Plaintiff Clawson places significant value in the security of his PII. Plaintiff Clawson entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Clawson has already suffered injury and remains at a substantial and imminent risk of future harm.

Texas

Michael Crain

86. Plaintiff Michael Crain is a resident of the State of Texas and is a current customer of AT&T's Wireless service. Plaintiff Crain is a former customer of AT&T's HBO service. As a condition of receiving services from AT&T, Plaintiff Crain provided AT&T with multiple types of PII. Plaintiff Crain was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Crain confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. Plaintiff Crain pays for his AT&T services using his checking account in conjunction with

AT&T's AutoPay. After the AT&T-Direct Data Breach, Plaintiff Crain received notice that his PII was found on the Dark Web. Additionally, Plaintiff Crain received and continues to receive incredible amounts of spam calls on the same phone number associated with his AT&T account. As a result of the AT&T-Direct Data Breach, Plaintiff spent significant time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including changing his passwords, initiating two factor authorization for his financial accounts, initiating fraud alerts for his accounts, and subscribing to ID Notify for identity protection through TurboTax. Plaintiff Crain places significant value in the security of his PII. Plaintiff Crain entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Crain has already suffered injury and remains at a substantial and imminent risk of future harm.

Yajaira De La Espada

87. Plaintiff Yajaira De La Espada is a resident of the State of Texas and is a former customer of AT&T's Wireless, Home Internet, and U-Verse, services. Plaintiff De La Espada is a current customer of AT&T's HBO Max service. As a condition of receiving services from AT&T, Plaintiff De La Espada provided AT&T with multiple types of PII. In connection with her use of AT&T's telecommunication services, AT&T collected and stored her call and text records and cell site identification numbers. Plaintiff De La Espada was notified by AT&T that her PII was compromised in both the AT&T-Direct and the AT&T-Snowflake Data Breaches. Plaintiff De La Espada confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct

Data Breach, Plaintiff De La Espada was notified about attempted unauthorized activity on her Bank of America checking account. This was the same account Plaintiff De La Espada set up on AutoPay for her AT&T services. Plaintiff De La Espada also had an unauthorized user attempt to log in to her Venmo account in 2022. Additionally, Plaintiff De La Espada received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct and AT&T-Snowflake Data Breaches, Plaintiff De La Espada spent time and effort researching the Data Breaches and monitoring her accounts for fraudulent activity, including closing her compromised Bank of America account and opening a new account, changing her passwords, initiating two-factor authentication for her accounts, initiating fraud alerts for her accounts, subscribing to Experian for approximately \$30 per month, and exercising additional vigilance about spam calls and messages that may be tied to information learned from the exposed call and text records. Plaintiff De La Espada also incurred late fees for services that were set up for payment with the compromised Bank of America account. Plaintiff De La Espada places significant value in the security of her PII. Plaintiff entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Plaintiff De La Espada also places significant value on the privacy and security of her call, text, and location information. This information reveals personal connections, relationships, and movements that Plaintiff De La Espada reasonably expected to remain private. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff De La Espada has already suffered injury and remains at a substantial and imminent risk of future harm.

Corrie Mueller

88. Plaintiff Corrie Mueller is a resident of the State of Texas and is a former customer of AT&T's DirecTV, Landline, U-Verse, and Home Internet services. Plaintiff Mueller is a current customer of AT&T's Wireless and HBO services. As a condition of receiving services from AT&T, Plaintiff provided AT&T with multiple types of PII. Plaintiff Mueller was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Mueller confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the Data Breach, Plaintiff Mueller experienced multiple unauthorized fraudulent charges on her Wells Fargo bank account, which is the same account she used to pay for her AT&T services and was a saved payment method in her AT&T account. Plaintiff Mueller also received a fraud alert from Experian and discovered information on her credit report she did not authorize or initiate. This unauthorized information lowered Plaintiff Mueller's credit score. Plaintiff Mueller also often receives unprompted alerts providing one-time two-factor authentication codes for her accounts with Amazon and Microsoft 365. This activity indicates that an unknown and unauthorized individual is attempting to log in to her accounts without her authorization or approval. Also, after the AT&T-Direct Data Breach, Plaintiff Mueller received a notice from Experian that her PII was found on the Dark Web. Additionally, Plaintiff Mueller received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address she provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Mueller spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including closing her compromised account, changing her passwords, initiating two-factor authentication for her accounts, freezing

her credit, initiating fraud alerts for her accounts, and subscribing to Experian for \$29.99 per month. Plaintiff Mueller has experienced significant stress as a result of the Data Breach and its interference with her life. Its impact on her personal information and credit was particularly stressful when she attempted to purchase a home and was aware that her financial information was vulnerable. Plaintiff Mueller places significant value in the security of her PII. Plaintiff Mueller entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Mueller has already suffered injury and remains at a substantial and imminent risk of future harm.

Ja’Vondrick Orange

89. Plaintiff Ja’Vondrick Orange is a resident of the State of Texas and is a current customer of AT&T’s DirecTV, Wireless, Home Internet, and HBO services. Plaintiff Orange is a former customer of AT&T’s U-Verse service. As a condition of receiving services from AT&T, Plaintiff Orange provided AT&T with multiple types of PII. Plaintiff Orange was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Orange confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, two of Plaintiff Orange’s checking accounts that were used to pay for his AT&T services experienced unauthorized charges. The unauthorized charges on one of Plaintiff Orange’s checking accounts resulted in unreimbursed expenses associated with missed payments to his other service providers. Additionally, Plaintiff Orange received and continues to receive incredible

amounts of spam calls, texts and emails on the phone numbers and email address associated with his AT&T services. As a result of the AT&T-Direct Data Breach, Plaintiff Orange spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including working with his banks to reissue debit cards, reverse overdraft fees, and refund unauthorized charges, changing his passwords, initiating two-factor authentication for his accounts, and freezing his credit. Plaintiff Orange places significant value in the security of his PII. Plaintiff Orange entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Orange has already suffered injury and remains at a substantial and imminent risk of future harm.

Utah

Charles Leonard

90. Plaintiff Charles Leonard is a resident of the State of Utah and is a former customer of AT&T's DirecTV, Wireless, Landline, Home Internet, and U-Verse services. As a condition of receiving services from AT&T, Plaintiff Leonard provided AT&T with multiple types of PII. Plaintiff Leonard was notified by AT&T that his PII was compromised in the AT&T-Direct Data Breach. Plaintiff Leonard confirmed that his PII—including his name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Leonard experienced unauthorized charges posted to his personal financial accounts with Capital One and received a notification from Credit Wise that an unknown and unauthorized individual was attempting to use his personal information. Also, after

the AT&T-Direct Data Breach, Plaintiff Leonard received notice that his PII was found on the Dark Web. Additionally, Plaintiff Leonard received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address he provided to AT&T. As a result of the AT&T-Direct Data Breach, Plaintiff Leonard spent time and effort researching the Data Breach and monitoring his accounts for fraudulent activity, including changing the passwords to his personal accounts, freezing his credit, consolidating his credit cards, checking his credit statements after every purchase and spending hours reviewing his personal financial information. Plaintiff Leonard places significant value in the security of his PII. Plaintiff Leonard entrusted his sensitive PII to AT&T with the understanding that AT&T would keep his PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Leonard has already suffered injury and remains at a substantial and imminent risk of future harm.

Virginia

Kayla Lee

91. Plaintiff Kayla Lee is a resident of the Commonwealth of Virginia and is a former customer of AT&T's Home Internet service. Plaintiff Lee is a current customer of AT&T's HBO service. As a condition of receiving services from AT&T, Plaintiff Lee provided AT&T with multiple types of PII. Plaintiff Lee was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Lee confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public web. After the AT&T-Direct Data Breach, Plaintiff Lee had unauthorized charges made on her

Chase Bank credit card account. Chase would not refund one of the fraudulent charges totaling \$423.14 that Plaintiff Lee was ultimately responsible for. Also, after the AT&T-Direct Data Breach, Plaintiff Lee received notice that her PII was found on the Dark Web. Additionally, Plaintiff Lee received and continues to receive incredible amounts of spam calls, texts and emails on the same phone number and email address associated with her AT&T services. As a result of the AT&T-Direct Data Breach, Plaintiff Lee spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including reissuing a credit card for her compromised account, changing her passwords, initiating two-factor authentication for her accounts, freezing her credit, initiating fraud alerts for her accounts, and subscribing to spam blocking services through her wireless cell phone provider. Plaintiff places significant value in the security of her PII. Plaintiff Lee entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Lee has already suffered injury and remains at a substantial and imminent risk of future harm.

Azima Sharrieff

92. Plaintiff Azima Sharrieff is a resident of the Commonwealth of Virginia and is a former customer of AT&T's Wireless, Prepaid, and Home Internet services. As a condition of receiving services from AT&T, Plaintiff Sharrieff provided AT&T with multiple types of PII. Plaintiff Sharrieff was notified by AT&T that her PII was compromised in the AT&T-Direct Data Breach. Plaintiff Sharrieff confirmed that her PII—including her name, date of birth, Social Security number, phone number, email address, and home address—was in the AT&T data extracted by an unauthorized third party and subsequently posted on both the dark web and public

web. After the AT&T-Direct Data Breach, Plaintiff Sharrieff had unauthorized charges on the checking account that was previously set up on AutoPay for her AT&T services. Similarly, an unknown and unauthorized individual successfully withdrew approximately \$2,700 from the same checking account that was set up on AutoPay with AT&T. Also, after the AT&T-Direct Data Breach, Plaintiff Sharrieff received notice that her PII was found on the Dark Web. Additionally, Plaintiff Sharrieff received and continues to receive incredible amounts of spam emails on the same email address she provided to AT&T. Plaintiff Sharrieff previously received such an incredible amounts of spam calls and texts on the phone number she provided to AT&T that she filed a police report and changed her phone number. As a result of the AT&T-Direct Data Breach, Plaintiff Sharrieff spent time and effort researching the Data Breach and monitoring her accounts for fraudulent activity, including replacing her debit card, changing her passwords, and initiating two-factor authentication for her accounts. Plaintiff Sharrieff places significant value in the security of her PII. Plaintiff Sharrieff entrusted her sensitive PII to AT&T with the understanding that AT&T would keep her PII secure and employ reasonable and adequate security measures to ensure that it would not be compromised. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Sharrieff has already suffered injury and remains at a substantial and imminent risk of future harm.

FACTUAL BACKGROUND

A. AT&T COLLECTS AND STORES ITS CURRENT AND FORMER CUSTOMER'S PERSONAL AND SENSITIVE INFORMATION

93. AT&T is a U.S. telecommunications and technology services provider that is publicly traded and operates for the profit and financial benefit of its shareholders. In North America, AT&T's network covers over 438 million people with 4G LTE. In the U.S., AT&T's network covers all major metropolitan areas and more than 334 million people with its LTE

technology and more than 302 million people with 5G technology. As of December 31, 2023, AT&T served 242 million AT&T Mobility subscribers and, with respect to Cingular Wireless, provided broadband and internet services to approximately 15 million customer locations.²⁰

94. In their Consumer Service Agreement, AT&T requires that all consumers seeking to use AT&T services agree to a set of universal terms, and that the consumer provide at the outset certain “identifiers” or unique information that is used to confirm an individual’s identity. These identifiers include an individual’s name, Social Security number, driver’s license number, phone number, financial information, and other identifying information unique to an individual, and must be provided for each service the consumer purchases or uses.²¹

95. AT&T collects and maintains the millions of consumer identifiers, and continues to maintain, develop, and utilize such identifiers even after a consumer discontinues using AT&T services.

96. In addition to collecting individual identifiers, the AT&T Privacy Notice provides that, by virtue of operating one of the nation’s largest telecommunications companies, AT&T has access to, collects, analyzes, and maintains other personal and sensitive information which is linked to the consumer’s identifiers (*i.e.*, consumer name, social security number, account, device),²² including:

- Customer Proprietary Network Information (or CPNI)
- Precise Geolocation (they know where you are)
- Demographic, religious or occupational information

²⁰ Annual Report Pursuant to Section 13 OR 15(d) of the Securities Exchange Act of 1934 (Form 10-K) (Feb. 23, 2024), <https://investors.att.com/~media/Files/A/ATT-IR-V2/t-2023-12-31-10k-2024.pdf>.

²¹ See AT&T Consumer Service Agreement; 1.1, <https://www.att.com/legal/terms.consumerServiceAgreement.html>; <https://about.att.com/privacy/privacy-notice/state-disclosures.html#sensitive-personal-info>.

²² See AT&T Privacy Notice, *supra* note 22.

- Racial or ethnic origin
- Religious or philosophical beliefs
- Union Membership
- Content of communications (up to 48 hours)
- Biometric information (i.e., voice prints, face scans, finger prints)
- Financial accounts & credentials
- Addresses (physical and email)
- Social Security number
- Driver's license number
- Passport number
- Device IDs
- Age
- Gender
- Preferred language
- Marital status
- Records of personal property
- Products or services purchased, obtained, or considered
- IP address
- Purchasing or consuming histories or tendencies
- Browsing history
- Search history (what search terms a customer enters)
- Information regarding the customers' interaction with an internet website, application, or advertisement
- Time consumers spend on websites or applications
- Links and ads seen
- Videos a consumer watches
- Items placed in online shopping carts
- Social media posts
- Individual profiles, preferences, characteristics, and behavior
- Degree(s), actual or inferred level of education
- Current or past employment history, licenses and professional Membership
- Video surveillance
- Audio recordings
- Photographs
- Signatures associated with an account
- People whom the consumers have called²³

²³ Personal Information Collected, AT&T, <https://about.att.com/privacy/privacy-notice/state-disclosures.html#we-collect> (Apr. 29, 2025).

97. What AT&T does not state is that it keeps personal and sensitive information for current and *former* consumers as long as it needs it for *whatever* business purposes.²⁴ In fact, many victims of the Data Breach were *former* AT&T customers.

98. AT&T has provided false hope to customers regarding the privacy of their data. In the Privacy Center, AT&T states that “[o]ur Privacy Principles are fundamental to our business, and reflect our commitment to” the following principles:²⁵



Transparency

We’re open and honest about how we use your data.



Choices & Controls

We give you choices about how we use your data.



Security

We use strong safeguards to keep your data safe and secure



Integrity

We do what we say.

99. AT&T states that it “is committed to fulfilling [its] responsibilities related to the collection, retention, use, and other processing of personal data” and promises that it “has implemented measures designed to secure personal data and to prevent unauthorized or accidental

²⁴ AT&T Privacy Notice, *supra* note 22. See also Consumer Service Agreement, §1.9.1, available at <https://www.att.com/legal/terms.consumerServiceAgreement.html> (“We also may share information about your credit with “AT&T’s current and future affiliates, assignees, successors, employees, agents, and others acting or purporting to act on our behalf at any time and for any reason.””).

²⁵ AT&T Privacy Center, Our Privacy Approach, AT&T, <https://about.att.com/privacy.html> (last visited Apr. 28, 2025).

access, erasure, or other misuse.”²⁶ In addition, AT&T claims to have a “state law approach” to data privacy and promises customers that it “will comply with all state laws” regarding same.²⁷

100. According to its 2023 Form 10-K, AT&T maintains “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.” AT&T further stated that its scientists and engineers conduct research in a variety of areas, including network and cybersecurity.

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

B. AT&T HAS A HISTORY OF MISMANAGING AND FAILING TO PROTECT SENSITIVE AND PERSONAL CONSUMER INFORMATION

102. The Data Breach and resulting harm suffered by Plaintiffs and Class Members is directly attributable to AT&T’s security lapses and data mismanagement. AT&T is no stranger to cybersecurity incidents resulting from the insecure collection, use, and sale of sensitive and personal customer information and customer identifiers. Despite these repeated breaches of its data systems, including the one giving rise to this litigation, AT&T appears to have taken no meaningful action to curtail further breaches, despite its assurances that to customers that it will keep their data secure.²⁸

²⁶ AT&T Privacy Center, Our Global Approach, AT&T, https://about.att.com/privacy/global_approach.html (last visited Apr. 28, 2025).

²⁷ AT&T Privacy Center, State Law Approach, AT&T, <https://about.att.com/privacy/state-law-approach.html> (last visited Apr. 28, 2025).

²⁸ AT&T Privacy Center, Our Privacy Approach, *supra* note 31; AT&T Privacy Center, Our Global Approach, *supra* note 32; AT&T Privacy Center, State Law Approach, *supra* note 33.

1. AT&T Data Breaches in 2023-2024 Demonstrate Flawed Security Measures and Corporate Mismanagement of Customer Personal Sensitive Information

103. AT&T reported another major breach that occurred in January 2023, during which hackers exploited flaws in the company's cloud systems, exposing sensitive data of nearly 9 million wireless customers. The breach included personal and account information and led to yet another investigation by the FCC as to how AT&T manages its cybersecurity and vendor relationships.

104. In September 2024, following the FCC's investigation into the January 2023 AT&T data breach, AT&T entered into yet another Consent Decree with the FCC (the "2024 Consent Decree"). The FCC familiarly concluded that "AT&T failed to ensure its vendor adequately protected that customer information; instead, it remained in the vendor's cloud environment for many years after it should have been deleted or returned to AT&T and was ultimately exposed in the 2023 Breach."²⁹

105. Less than three weeks after AT&T announced its investigation into the AT&T-Direct Data Breach, AT&T discovered a second cybersecurity incident caused by the same Threat Actor originating with its vendor, Snowflake Inc. (the "AT&T-Snowflake Breach"). This second incident, discussed further below, compromised records of calls and texts of nearly all of AT&T's wireless customers from May 1, 2022, to October 31, 2022. AT&T announced this incident on July 12, 2024.

106. According to AT&T, the data stolen in the AT&T-Snowflake Breach "does not contain the content of calls or texts," but does include calling and texting records that an AT&T

²⁹ See *In the Matter of AT&T Services Inc.*, File No. EB-TCD-23-00034851 (F.C.C. Sep. 17, 2024).

phone number interacted with during the six-month period, as well as the total count of a customer's calls and texts, and call durations. Some of the stolen records include cell site identification numbers associated with phone calls and text messages, information that can be used to determine the approximate location of where a call was made or text message sent.

107. A security expert highlighted that the potential for triangulation of customers' locations from compromised cell site identification numbers, along with the information exposed in the AT&T-Snowflake Data Breach (*i.e.*, names, addresses, birth dates, Social Security Numbers, etc.), "adds a physical dimension to the already extensive privacy violation and could expose individuals to highly targeted and convincing social engineering attacks, not to mention compromising [their] physical security. . . ." ³⁰

108. Then, in October 2024, the Wall Street Journal announced a *third* breach of AT&T data—naming AT&T among broadband providers that were breached in a cyberattack tied to the Chinese government. Hackers penetrated the networks of a swath of U.S. broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests ("Salt Typhoon Breach"). ³¹ And while the Salt Typhoon Breach was reported as being perpetrated by hackers acting on behalf of a nation state, it is unsurprising that

³⁰ Nate Nelson, *AT&T Breach May Also Impact Millions of Boost, Cricket, H2O Customers*, DARK READING (July 12, 2024), <https://www.darkreading.com/cyberattacks-data-breaches/att-breach-may-also-impact-millions-of-boost-cricket-h2o-customers>.

³¹ Sarah Krouse, Dustin Volz, Aruna Viswanatha, and Robert McMillan, *U.S. Wiretap Systems Targeted in China-Linked Hack*, THE WALL STREET JOURNAL (Oct. 5, 2024), <https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b>.

AT&T was a target given its two prior leaks in 2024. These other 2024 breaches were attributed to the threat actor ShinyHunters, a group composed of individual criminals.³²

109. Nor has AT&T informed its customers of the Salt Typhoon Data Breach. According to news sources, hackers' access gave them "the capability to geolocate millions of individuals" as well as "to record phone calls at will[.]"³³

2. AT&T Discloses Its Second Major Breach of Customer Data In 2024

110. On July 12, 2024, AT&T publicly announced that data of "nearly all" its 110 million cellular customers from May 1, 2022 to October 31, 2022 and January 2, 2023 was illegally downloaded from its workspace on a third-party [Snowflake's] cloud platform.³⁴

111. According to AT&T, the stolen data in the AT&T-Snowflake Data Breach includes calling and texting records that an AT&T phone number interacted with during the six-month period, as well as the total count of a customer's calls and texts, and call durations — information that is known as metadata. It also includes other phone numbers that an AT&T wireless number interacted with during this time, including AT&T landline customers.³⁵

112. AT&T stated "[t]he downloaded data doesn't include the content of any calls or texts. It doesn't have the time stamps for the calls or texts. It also doesn't have any details such as

³² Annika Burgess, *What we know about the 'remarkably devious' ShinyHunters hackers allegedly behind the Ticketmaster data leak*, ABC NEWS (May 30, 2024), <https://www.ABC.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928>.

³³ Matthew J. Schwartz, *AT&T and Verizon Say Chinese Hackers Ejected from Network*, BANKINFOSECURITY (Dec. 31, 2024), <https://www.bankinfosecurity.com/att-verizon-say-chinese-hackers-ejected-from-networks-a-27190>.

³⁴ *AT&T Addresses Illegal Download of Customer Data*, AT&T (July 12, 2024), <https://about.att.com/story/2024/addressing-illegal-download.html>

³⁵ *Id.*

Social Security numbers, dates of birth, or other personally identifiable information. [¶] While the data doesn't include customer names, there are often ways to find a name associated with a phone number using publicly available online tools.”³⁶

113. The AT&T-Snowflake Data Breach also includes a subset of records from January 2, 2023. For this subset of records, one or more cell site ID numbers associated with the phone calls and text messages were also breached.³⁷ This is information that can be used to determine the approximate location of where a call was made or text message was sent.

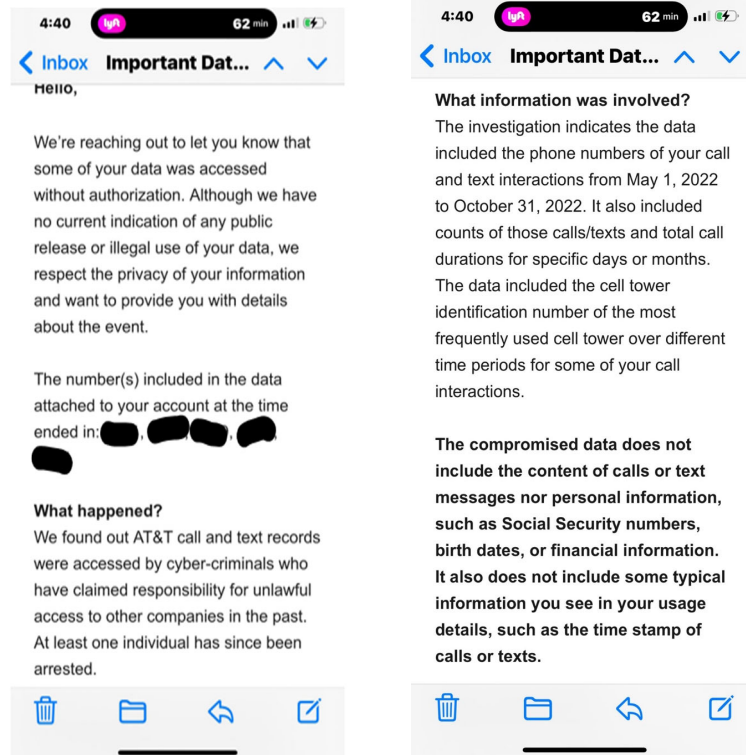
114. The stolen data also includes call and text records of customers with phone service from other cell carriers that rely on AT&T's network - mobile virtual network operators or MVNOs. According to public sources, those MVNOs likely include wireless service providers such as Boost Mobile.³⁸

115. On July 12, 2024, AT&T began notifying Plaintiff and Class Members of the AT&T-Snowflake Data Breach via electronic mail:

³⁶ *Id.*

³⁷ *Id.*

³⁸ Max McCaskill, *AT&T MVNOs: Carriers that use AT&T's network*, WHISTLEOUT (Nov. 25, 2024), <https://www.whistleout.com/CellPhones/Guides/att-mvnos>.



116. In a July 12, 2024 SEC filing AT&T provided even more details of the AT&T-Snowflake Data Breach. In its Form-8K disclosing a material cybersecurity incident AT&T explained:

On April 19, 2024, AT&T Inc. (“AT&T”) learned that a threat actor claimed to have unlawfully accessed and copied AT&T call logs. [] Based on its investigation, AT&T believes that threat actors unlawfully accessed an AT&T workspace on a third-party cloud platform and, between April 14 and April 25, 2024, exfiltrated files containing AT&T records of customer call and text interactions that occurred between approximately May 1 and October 31, 2022, as well as on January 2, 2023, as described below . . .

.

Current analysis indicates that the data includes, for these periods of time, records of calls and texts of nearly all of AT&T’s wireless customers and customers of mobile virtual network operators (“MVNO”) using AT&T’s wireless network. These records identify the telephone numbers with which an AT&T or MVNO wireless number interacted during these periods, including telephone numbers of AT&T wireline customers and customers of other carriers, counts of those interactions, and aggregate call duration for

a day or month. For a subset of records, one or more cell site identification number(s) are also included. While the data does not include customer names, there are often ways, using publicly available online tools, to find the name associated with a specific telephone number.

... ..

On May 9, 2024, and again on June 5, 2024, the U.S. Department of Justice determined that, under Item 1.05(c) of Form 8-K, a delay in providing public disclosure was warranted. AT&T is now timely filing this report. AT&T is working with law enforcement in its efforts to arrest those involved in the incident. Based on information available to AT&T, it understands that at least one person has been apprehended. As of the date of this filing, AT&T does not believe that the data is publicly available.³⁹

117. On July 12, 2024, AT&T stated the access point had been secured, it did not believe the data was publicly available, and at least one person had been apprehended.⁴⁰

118. An AT&T spokesperson confirmed that the data was exposed “on ‘AI data cloud’ provider Snowflake[.]”

119. Snowflake provides digital warehouses, known as “Snowflake Data Clouds” for its clients, such as AT&T, and as a result has access to, stores, and maintains huge datasets of Private Information of AT&T’s corporate clients’ customers and employees.

120. In or around mid-April 2024, an unauthorized party or parties gained access to Snowflake’s customer accounts stealing customer and employee data from AT&T and others.

121. The AT&T-Snowflake Data Breach was perpetrated by a cybercriminal group known as UNC5537, the same group responsible for breaching other companies’ data stored on Snowflake’s cloud platform.

³⁹ United States Securities and Exchange Commission (Form 8-K)(May 6, 2024), <https://otp.tools.investis.com/clients/us/atnt2/sec/sec-show.aspx?FilingId=17677638&Cik=0000732717&Type=PDF&hasPdf=1>.

⁴⁰ *AT&T Addresses Illegal Download of Customer Data*, *supra* note 71.

122. UNC5537 is a financially motivated threat actor group likely comprised of hackers based in North America and Turkey. The group employs information-stealing malware to infiltrate systems, collect user data, and then sell it on underground cybercrime forums or to other hackers.

123. According to cybersecurity experts, UNC5537's attack was "not the result of any particularly novel or sophisticated tool, technique, or procedure" but was instead the consequence of "missed opportunities" to properly secure credentials.

124. UNC5537's attack method consisted of obtaining AT&T's Snowflake credentials (username and password) and simply using those credentials to log into AT&T's Snowflake account and exfiltrate customer data. Many of the credentials used by UNC5537 were old and had been acquired from malware campaigns dating back to 2020.

125. Mandiant revealed that the threat campaign was successful because "the impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password."⁴¹

126. MFA is a simple yet robust security system that requires more than one method of authentication from independent categories of credentials (*e.g.*, a username/password and confirmation link sent via email).

127. Infamous threat actors, known by the handle "ShinyHunters," boasted to journalists that the Data Breach was enabled by the lack of MFA enforcement.⁴²

128. MFA administrator enforcement is the industry standard, according to Ofer Maor,

⁴¹ *Id.*

⁴² Kim Zetter, *Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake*, WIRED (Jun. 17, 2024), <https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/>.

cofounder and Chief Technology Officer of data security investigation firm Mitiga.⁴³ He notes that “most SaaS (soft-as-a-service) vendors, once deployed as an enterprise solution, allow administrators to enforce MFA... they require every user to enroll in MFA when they first login and make it no longer possible for users to work without it.” A data security firm’s principal simply noted it is “surprising that the built-in account management within Snowflake doesn’t have more robust capabilities like the ability to enforce MFA.”⁴⁴

129. Snowflake blames the data thefts on its customers – such as AT&T here, who did not require MFA to secure their Snowflake accounts. Indeed, AT&T’s failure to implement the most basic cybersecurity features, including MFA, was, at minimum, a substantial factor in causing this Data Breach.

130. AT&T, as a telecommunications provider, is well-familiar with MFA⁴⁵ and knows that implementation of certain basic security measures of this kind are critical to protecting sensitive information. According to AT&T, “[t]he majority of data breaches are caused by brute

⁴³ Solomon Klappholz, *With hundreds of Snowflake credentials published on the dark web, it’s time for enterprises to get MFA in order*, ITPRO (Jun. 7, 2024), <https://www.itpro.com/security/cyber-attacks/with-hundreds-of-snowflake-credentials-published-on-the-dark-web-its-time-for-enterprises-to-get-mfa-in-order>.

⁴⁴ Shane Snider, *Snowflake’s Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, INFORMATION WEEK (June 5, 2024), <https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say>.

⁴⁵ Indeed, AT&T is credited as having invented MFA three decades ago, holding a patent for a “transaction authorization and alert system” that allowed customers to authorize transactions through the use of a messaging or alert system. AT&T Corp., Transaction authorization and alert system, P0745961 (A2), https://worldwide.espacenet.com/publicationDetails/biblio?DB=worldwide.espacenet.com&II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=19961204&CC=EP&NR=0745961A2&KC=A2; Jon Brodtkin, Kim Dotcom claims he invented two-factor authentication—but he wasn’t the first, ArsTechnica (May 23, 2013), <https://arstechnica.com/information-technology/2013/05/kim-dotcom-claims-he-invented-two-factor-authentication-but-he-wasnt-first/>.

force attacks on credentials.”⁴⁶ AT&T even has its own MFA application, AT&T MFA, which it describes as “a next-generation” solution for the latest protection.”⁴⁷

131. In addition, AT&T is well-aware of other basic data security measures, including rotating or disabling old credentials and limiting access to trusted locations and/or users.

132. Yet AT&T did not take any of these rudimentary measures to ensure that the sensitive information located on Snowflake’s cloud was fully protected. Had AT&T implemented a policy to enable and require MFA, rotate or disable old credentials, and/or limit access to trusted locations and/or users, this Data Breach could have been thwarted at an earlier stage or averted altogether.

C. AT&T FAILED TO PROTECT FORMER AND CURRENT CUSTOMERS’ SENSITIVE PERSONAL INFORMATION

1. AT&T’s Systems Were Compromised by ShinyHunters, and Personal Identifying Information of Over 70 Million Customers Was Exfiltrated and Posted on the Dark Web

133. At the same time that AT&T collected, stored, and profited from consumers’ personal information and identifiers, it permitted a massive data breach compromising the PII of millions of its customers.

134. When first presented with evidence of the AT&T-Direct Data Breach, however, AT&T denied that it occurred. According to media sources, customer PII from the AT&T-Direct Data Breach first appeared for sale nearly three years ago in August 2021 on the dark web, when

⁴⁶ *Secure Access to Your Corporate Network and Prevent Identity Fraud with AT&T Multi-Factor Authenticator*, AT&T BUSINESS, <https://cdn-cybersecurity.att.com/docs/product-briefs/att-multi-factor-authenticator.pdf> (last visited Apr. 25, 2025).

⁴⁷ *Id.*

a known threat actor, ShinyHunters, posted for sale “AT&T Database +70M (SSN/DOB)” on a hacker forum and marketplace:⁴⁸

SELLING AT&T Database +70M (SSN/DOB)
by ShinyHunters - 2 hours ago

Pages (2): 1 2 Next »

2 hours ago · This post was last modified: 2 hours ago by ShinyHunters · Edited 2 times in total

ShinyHunters

GOD User

GOD

Posts: 84
Threads: 47
Joined: Apr 2020
Reputation: 2,244

1 YEAR OF SERVICE

Sample

Decrypted

Decrypted values are provided after purchase.

DOB:

.encrypted_value='*0GW5xfv74NGZ8rimVzA0zvA==' .decrypted_value='1971-04-12'
.encrypted_value='*0GW5xfv74NGaoCTxtH+Wh4g==' .decrypted_value='1971-04-13'
.encrypted_value='*0GW5xfv74NGbUwwMYdMRiaA==' .decrypted_value='1971-04-14'
.encrypted_value='*0GW5xfv74NGajDxMvzF+LMw==' .decrypted_value='1971-04-15'
.encrypted_value='*0GW5xfv74NGabSFT5QhD0FA==' .decrypted_value='1971-04-16'

SSN:

.encrypted_value='*102NB6y72cLc=' .decrypted_value='435624606'
.encrypted_value='*102nBA2G583E=' .decrypted_value='298693795'
.encrypted_value='*102nbbStErJE=' .decrypted_value='224731017'
.encrypted_value='*102NBsPqk4q8=' .decrypted_value='256781396'
.encrypted_value='*102nBTulxGIQ=' .decrypted_value='424250144'

Start: \$200k
Minimum step: \$30k
Flash: \$1kk

ShinyHunters later stated they would sell the database immediately for \$1 million.

135. The dark web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term “dark web” is used to distinguish from the “clear web,” the part of the World Wide Web that is readily accessible through traditional internet browsers. The

⁴⁸ 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/>.

dark web is accessed through The Onion Router (“Tor”), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers (relays), encrypting data at each step to ensure that both the user’s location and browsing activity are difficult to trace. Tor uses a technique called “onion routing,” where data is encrypted in layers like an onion. Each relay in the network peels away a layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

136. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence. The anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen PII.⁴⁹

137. Once stolen PII is posted on the dark web, it will most likely be distributed to multiple different groups and individuals, each of which can use that information for fraud and identity theft.⁵⁰

138. This data lifecycle has also been confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then “watermarked” it

⁴⁹ *Crime and the Deep Web*, STEVENSON UNIV., <https://www.stevenson.edu/online/about-us/news/crime-deep-web/> (last visited Apr. 26, 2025); *Defending Against Malicious Cyber Activity Originating from Tor*, CISA, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a> (last updated Aug. 2, 2021).

⁵⁰ *The Dark Web and Cybercrime*, U.S. DEP’T OF HEALTH AND HUMAN SERVS. (July 23, 2020), <https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf>.

with their code that silently tracks any access to the file.⁵¹ The data was quickly spread across five continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and Brazil, with the most activity coming from Nigeria and Russia.⁵² This experiment demonstrated that data released on the dark web will quickly spread around the world.

139. *Hackread*, one of the technology sites that reported the auctioning of the data online, noted that it “has seen the sample records shared by ShinyHunters on the forum” and that a “review of it reveals that these records include the following customers’ details: [f]ull names, [a]ddresses, [z]ipcodes, [d]ate of birth, [e]mail addresses and Social Security numbers (SSN).⁵³

140. Despite the fact that the hackers selling the data advertised it as coming from the “AT&T Database,” AT&T denied that it had been breached. In a statement to *Hackread* and other media sources AT&T denied being breached: “Based on our investigation today, the information that appeared in an internet chat room does not appear to have come from our systems.”⁵⁴ Three years later, however, AT&T was forced to admit that the data did come from its systems.

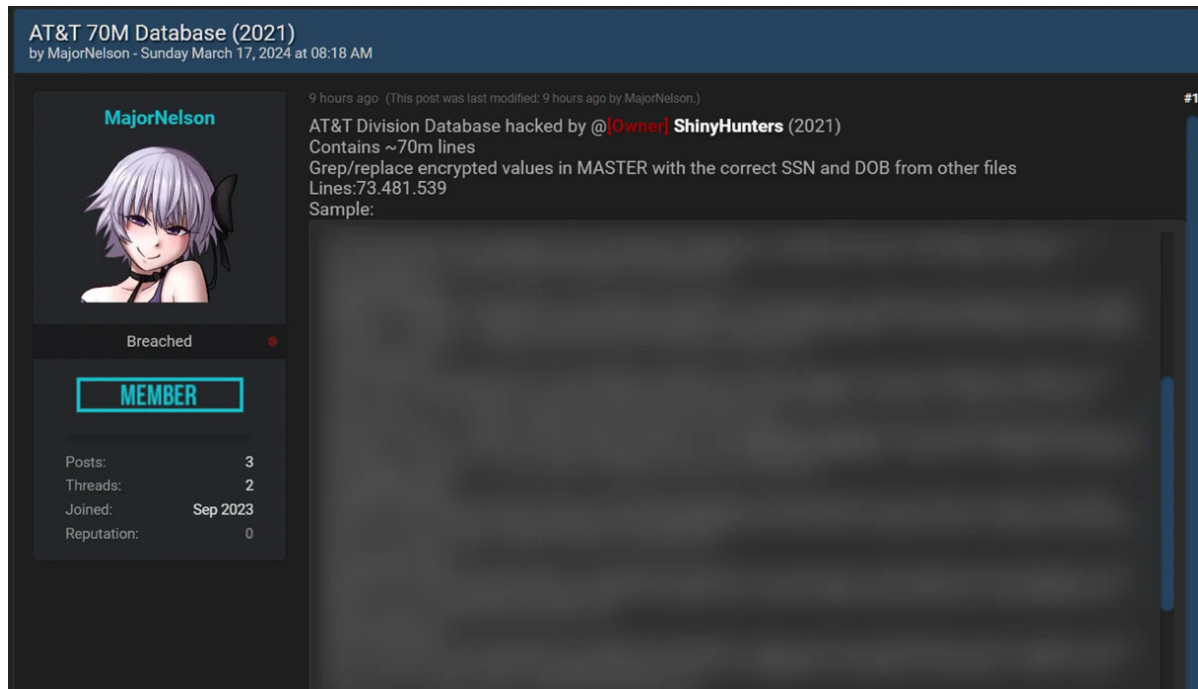
⁵¹ Kelly Jackson Higgins, *What Happens When Personal Information Hits the Dark Web*, DARK READING (Apr. 7, 2015), <https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web>; Kristin Finklea, *Dark Web*, NAT’L SEC. ARCHIVE (July 7, 2015), <https://nsarchive.gwu.edu/media/21394/ocr>; *Dark Web*, CONGRESSIONAL RESEARCH SERVICE, <https://crsreports.congress.gov/product/pdf/R/R44101> (last updated Mar. 10, 2017).

⁵² Pierluigi Paganini, *How Far Do Stolen Data Get in the Deep Web After a Breach?*, SECURITY AFFAIRS (Apr. 12, 2015), <https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html>.

⁵³ *Id.*

⁵⁴ Waqas, *supra* note 89; Lawrence Abrams, *AT&T denies data breach after hack auctions 70 million user database*, BLEEPING COMPUTER (Aug. 21, 2021), <https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/>.

141. On March 17, 2024, the leaked data appeared for sale again, this time by in another threat actor known as MajorNelson, who posted the compromised data for free on a hacking forum database, claiming it was the data ShinyHunters attempted to sell in 2021:⁵⁵



142. This new post revealed that the customer information included AT&T account-specific information, which meant that AT&T could no longer credibly deny that its systems had been compromised.

143. On or about March 30, 2024, AT&T publicly announced that the details of 73 million former and current AT&T customer accounts, including its customers' personally identifiable information and AT&T account numbers and passcodes, were leaked on the Dark Web.⁵⁶

⁵⁵ Lawrence Abrams, *AT&T says leaked data of 70 million people is not from its systems*, BLEEPING COMPUTER (Mar. 7, 2024), <https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/>.

⁵⁶ *AT&T Address Recent Data Set Released on the Dark Web*, AT&T (Mar. 30, 2024), <https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html>.

144. AT&T's announcement, posted on its website stated:

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 operations⁵⁷

145. On April 11, 2024, AT&T began mailing notice of the AT&T-Direct Data Breach to impacted parties,⁵⁸ such as Plaintiffs and Class Members, but has otherwise released very little information about the Data Breach since that time.

146. After falsely denying that its systems were breached in August 2021, AT&T appears to have done nothing at all to protect its 73 million current and former customers from the effects of its negligence for the following nearly three years. AT&T now claims to have “launched a robust investigation supported by internal and external cybersecurity experts,” something it

⁵⁷ *Id.*

⁵⁸ See, e.g., AT&T Customer Notification Letter Template, available at <https://oag.ca.gov/system/files/Customer%20Notification%20Letter%20Template.pdf> (last visited Apr. 28, 2025).

should have done in 2021 to have any hope of actually mitigating the extensive harm its false denial has—and no doubt will—cause for years to come.

147. AT&T was familiar with its obligations—created by contract, industry standards, common law, and representations to its customers—to protect customer information. Plaintiffs and Class Members provided their PII to AT&T with the reasonable expectation that AT&T would comply with its obligations to keep such information confidential and secure.

148. AT&T failed to comply with these obligations, resulting in the AT&T-Direct Data Breach. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records.

2. ShinyHunters' Tactics Are Well Known in the Cybersecurity Industry

149. ShinyHunters is a notorious cybercriminal group that became widely known in 2020, gaining attention with high-profile data breaches.⁵⁹ ShinyHunters was first widely known for selling 91 million user records from the Indonesian e-commerce platform Tokopedia on the dark web.⁶⁰ Since then, they have targeted companies across various sectors, including technology, education, media, and e-commerce, accumulating a significant track record of breaches.

150. The group is known for its financially motivated operations, primarily involving the theft and sale of data. They have compromised several companies, such as Pixlr, NitroPDF, and MeetMindful, often leaking the stolen data on hacking forums either for free or for sale.

⁵⁹ Lily Hay Newman, *ShinyHunters Is a Hacking Group on a Data Breach Spree*, WIRED (May 21, 2020), <https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/>; *ShinyHunters, one of the most recognised threat actors among the hacking community*, WHITEBLUEOCEAN (Feb. 2, 2021), <https://www.whiteblueocean.com/newsroom/shinyhunters-one-of-the-most-recognised-threat-actors-among-the-hacking-community/>.

⁶⁰ *ShinyHunters*, BUGCROWD, <https://www.bugcrowd.com/glossary/shinyhunters/> (last visited Apr. 28, 2025).

ShinyHunters also appears to have links to the earlier hacking group GnosticPlayers, sharing similar tactics of staggered data dumps, although they deny any direct connection.

151. The name ShinyHunters appears to derive from the “shiny” blue Umbreon Pokémon, and the attackers use the Pokémon goal of “Catch ‘em all!”⁶¹ This threat actor group has disseminated data for sale through a variety of Dark Web forums. These forums have, at times, been shut down by the FBI, only to reemerge with a different Dark Web address.⁶² One such forum is shown here⁶³:



⁶¹ Annika Burgess, *supra* note 69.

⁶² Jai Vijayan, *Leak Site BreachForums Springs Back to Life Weeks After FBI Takedown*, DARK READING (May 29, 2024), <https://www.darkreading.com/cyberattacks-data-breaches/leak-site-breachforums-springs-back-to-life-weeks-after-fbi-takedown>.

⁶³ The URL for the dark web site, which is not accessible through traditional Internet browsers, is shown here: <http://darknet47w5otuw7koxrqgasuljjh6dhz7dw5iapmsekhjqbwipfpsad.onion/?p=586>.

152. ShinyHunters is known for targeting companies with large user bases. They exfiltrate data from these organizations and often post the data for sale on dark web marketplaces or underground forums.


153. ShinyHunters has targeted well-known platforms and services, typically those with weaker security measures, large user databases, or high-profile reputations. In some instances, ShinyHunters engages in ransom-based attacks, demanding payments to avoid leaking stolen data. If a target refuses to pay, the group typically releases or sells the stolen information. Unlike other groups that specialize in ransomware or advanced persistent threat tactics, ShinyHunters focuses on maximizing the volume of data they acquire and monetize. ShinyHunters also targets applications with weak API security, such as a lack of authentication or rate-limiting. By exploiting these weaknesses, they can access sensitive data through exposed API endpoints. Once they gain access to an organization's database, ShinyHunters uses APIs to retrieve sensitive data in bulk. This is especially common when organizations use cloud-hosted databases with inadequate access control.

154. ShinyHunters has a history of attacking developer repositories to steal credentials or API keys.⁶⁴ The group often begins by searching for companies using Microsoft Office 365 and third parties that store GitHub open authorizations tokens.⁶⁵ The threat actors then identify research

⁶⁴ Ravie Lakshmanan, *Researchers Detail Modus Operandi of ShinyHunters Cyber Crime Group*, THE HACKER NEWS (Aug. 31, 2021), <https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html>.

⁶⁵ *Researchers Share Common Tactics of ShinyHunters Threat Group*, DARK READING (Aug. 24, 2021), <https://www.darkreading.com/cyberattacks-data-breaches/researchers-share-common-tactics-of-shinyhunters-threat-group>.

and development employees in the organizations. The MITRE group has provided a graphic of ShinyHunters tactics:⁶⁶

ShinyHunters Scenario Most Likely Courses of Action	ShinyHunters Scenario Most Dangerous Courses of Action
RECONNAISSANCE [TA0043]	
<ul style="list-style-type: none"> Identify organizations using Microsoft Office 365 and search for valid accounts. 	<ul style="list-style-type: none"> Identify third-party companies that store GitHub open authorization (OAuth) tokens. Identify and research development and operations (devops) personnel.
WEAPONIZATION	
<ul style="list-style-type: none"> Identify credentials for valid accounts from leaked and/or previously stolen credential data sets. Purchase credentials on marketplaces such as Genesis. Use accounts to log in to cloud services. 	<ul style="list-style-type: none"> Hack third-party companies to steal OAuth tokens, leverage them to bypass two-factor authentication (2FA) and gain access to cloud services. Directly target devops personnel to phish valid GitHub repository credentials.
DELIVERY [TA0001]	
<ul style="list-style-type: none"> Directly target database vulnerabilities to access sensitive information. 	<ul style="list-style-type: none"> Target software repositories to access application programming interface (API) keys, OAuth keys, hard-coded credentials and more.
EXPLOITATION	
<ul style="list-style-type: none"> Steal sensitive data such as credentials and PII. Exploit remote service tools. 	<ul style="list-style-type: none"> Audit source code to find vulnerabilities that can be leveraged in larger scale attacks.
COMMAND AND CONTROL [TA0011]	
<ul style="list-style-type: none"> Exfiltrate data via web services. Alternate domain name system (DNS) records to redirect legitimate traffic. Use exploited nodes as a vector and/or exit node for future attacks. 	<ul style="list-style-type: none"> Leverage legitimate credentials and tools such as GitHub utilizing OAuth which makes it more difficult to detect.
ACTIONS ON OBJECTIVES [TA0040]	
<ul style="list-style-type: none"> Sell stolen data on forums for profit. 	<ul style="list-style-type: none"> Extort, blackmail and expose information in the underground.
OUTCOME	
<ul style="list-style-type: none"> Confidentiality: Information theft and espionage. Integrity: Modification or deletion of data from an unauthorized party. Availability: Unable to update or access the environment until it is secured and accounts are reset. 	<ul style="list-style-type: none"> Confidentiality: Private information available publicly. Integrity: Modification or deletion of data from an unauthorized party. Availability: Unable to update or access the environment until it is secured and accounts are reset.
	

⁶⁶ Here's how to guard your enterprise against ShinyHunters, INTEL 471 (Aug. 23, 2021), <https://intel471.com/blog/shinyhunters-data-breach-mitre-attack>.

155. The TA0043 Reconnaissance refers to the MITRE groups description of reconnaissance techniques.⁶⁷

156. Once ShinyHunters gains access to a system, they exploit remote code execution vulnerabilities to execute arbitrary commands on vulnerable servers, gaining a foothold in the infrastructure. This often allows deeper access to network resources, expanding their reach to other parts of the organization.

157. ShinyHunters frequently leverages SQL injection attacks to gain unauthorized access to databases. By injecting malicious SQL queries into web application inputs (*e.g.*, login forms, search boxes, etc.), they manipulate the database to reveal sensitive information.

158. ShinyHunters often employs phishing attacks. These attacks depend on tricking a user to click on a link or open an attachment. ShinyHunters will often set up fake websites that purport to be real websites and send phishing emails attempting to lure recipients to the fake website. When the user logs in to the fake website, the attackers now have that user's credentials.⁶⁸ For example, the phishing email might purport to be from the cloud provider asking the recipient to click on a link or open some attached document. This would allow the attacker to get that users credentials for initial access to the cloud repository.

159. According to Skyhigh Security,⁶⁹ the typical ShinyHunters modus operandi includes:

⁶⁷ *Reconnaissance*, MITRE, <https://attack.mitre.org/tactics/TA0043/> (last visited: Apr. 28, 2025).

⁶⁸ Annika Burgess, *supra* note 69.

⁶⁹ Rodman Ramezani, *Ticketmaster's Encore: How "ShinyHunters" Hacked the Show*, SKYHIGH SECURITY (July 11, 2024), <https://www.skyhighsecurity.com/about/resources/intelligence-digest/ticketmasters-encore-how-shinyhunters-hacked-the-show.html>.

- **Orchestrating deception campaigns** by deploying sophisticated phishing schemes that aim to lure victims with fraudulent emails to capture login credentials.
- **Targeting unsecured cloud storage** to capitalize on poorly protected online data storage, which is akin to raiding unguarded digital vaults.
- **Infiltrating and compromising web platforms and development tools**, often purloining login details or application programming interface (API) keys to pilfer valuable data.
- **Probing GitHub repositories** to scrutinize company code repositories for exploitable flaws, potentially granting unauthorized database access.
- **Monetizing via covert networks** to profit by trading stolen data on obscure internet marketplaces, catering to buyers seeking illicit information.

160. ShinyHunters is active on the dark web, where they list data breaches for sale. They typically offer “exclusive” sales, where only one buyer receives the dataset, or “multi-buy” options, where the dataset is sold to several buyers. The group has carefully cultivated a reputation on forums, which makes buyers more likely to trust and purchase their listings. They provide “sample” data from breaches to verify authenticity, encouraging purchases by demonstrating the quality of data. If ransom demands are not met, ShinyHunters occasionally “leaks” data in a staged manner to maximize pressure on the victim. They sometimes release partial data as a warning, giving targets a chance to pay before the full release.

161. The cybersecurity journal Dark Reading,⁷⁰ reported the following data batches ShinyHunter was selling on the dark web in 2020:

⁷⁰ *ShinyHunters Offers Stolen Data on Dark Web*, DARK READING (July 28, 2020), <https://www.darkreading.com/cyberattacks-data-breaches/shinyhunters-offers-stolen-data-on-dark-web>.

- Vakina.com.br — 4.8 million records
- Truefire.com — 600,000 records
- Havenly.com — 1.3 million records
- Drizly.com — 2.4 million records
- Proctoru.com — 444,000 records
- Scentbird.com — 5.8 million records
- Appen.com — 5.8 million (suffered breach in 2017)
- Homechef.com — 8 million records
- Chatbooks.com — 15 million records

162. According to Forbes “In just the first two weeks of May 2020, a hacker, known only as ShinyHunters, offered an astonishing 200 million stolen data records for sale on the dark web. Not repurposed data from old breaches, but fresh to the market and, therefore, very valuable. The surprising thing is that, until then, nobody had even heard of ShinyHunters.”⁷¹

163. ShinyHunters is also known for simply giving away data. This has enhanced ShinyHunters’s reputation among cybercriminals and provides assurances that data offered for sale on the dark web is authentic and high quality.

164. ShinyHunters often uses IP rotation techniques and VPNs to mask their locations, making it difficult to track their activities or pinpoint their origin. This helps them stay anonymous and operate across jurisdictions without triggering alerts.

⁷¹ Davey Winder, *Hacker Gives Away 386 Million Stolen Records On Dark Web—What You Need To Do Now*, FORBES (July 29, 2020), <https://www.forbes.com/sites/daveywinder/2020/07/29/hacker-gives-away-386-million-stolen-records-on-dark-web-what-you-need-to-do-now-shinyhunters-data-breach/>.

165. The tactics, techniques, or procedures of ShinyHunters are well documented. It is reasonable to assume that the threat actor utilized one or more of the methods they have used in other attacks against AT&T.

3. AT&T Could Have (and Should Have) Secured Their Systems Against an Attack by ShinyHunters

166. Given that AT&T has not disclosed any details of the Data Breaches, remediation steps specific to that breach cannot be listed. However, given ShinyHunter's well established modus operandi, AT&T could have and should have taken steps that would have mitigated ShinyHunter's typical tactics and helped to prevent the breach.

167. The use of multi-factor authentication makes any data breach much more difficult to execute and can prevent a data breach caused by the compromise of user credentials. With the disclosure of the AT&T-Snowflake Data Breach, it has been reported that AT&T did not have multi-factor authentication in place.⁷² Had AT&T followed industry standards and used multi-factor authentication to prevent unauthorized use of user credentials, it would have helped to prevent the breach, slowed down the hackers, and potentially prevent the breach altogether. Multi-factor authentication is an industry standard and was in 2019.⁷³

⁷² Clay Wallace, *Two-factor authentication could have prevented AT&T data breach affecting 110 million customers*, WUKY (July 18, 2024), <https://www.wuky.org/local-regional-news/2024-07-18/two-factor-authentication-could-have-prevented-at-t-data-breach-affecting-110-million-customers>; Megan Leader, *Supply Chain Nightmare: AT&T-Snowflake Breach Is What Keeps CISOs Up at Night*, VIRTRU (July 12, 2024), <https://www.virtru.com/blog/cloud-security/att-snowflake-breach>.

⁷³ See, e.g., *NIST Special Publication 800-63B; Digital Identity Guidelines; Authentication and Lifecycle Management*, NIST (June 2017), <https://pages.nist.gov/800-63-3/sp800-63b.html>; NIST Update: Multi-Factor Authentication and SP 800-63 Digital Identity Guidelines, NIST (Feb. 15, 2022), https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf; *Require Multifactor*

168. When data is at rest, it should be encrypted. Encryption is insurance against data breaches because it prevents an unauthorized third party from exploiting stolen data, even if they gain access to it. Encryption at rest is commonly used to protect sensitive information like personal data, financial records, and intellectual property stored on devices or in cloud storage, reducing the risk of data breaches if the physical storage is stolen or compromised. Many data privacy regulations, such as GDPR, HIPAA, and PCI-DSS, require encryption at rest to protect sensitive data. AT&T recognizes the importance of encryption at rest, especially considering its job posting for a person who would be responsible for encrypting data at rest.⁷⁴ AT&T's cybersecurity division, LevelBlue, also tells its customers to encrypt cloud data at rest.⁷⁵ LevelBlue blogs recommend encrypting data at rest and in transit.⁷⁶ AT&T should have followed industry standards and properly encrypted sensitive PII at rest before the Data Breach occurred. Instead, AT&T left

Authentication, CISA, <https://www.cisa.gov/secure-our-world/require-multifactor-authentication> (last visited Apr. 28, 2025); *Multi-factor authentication: Key protection to tax professionals' security arsenal now required*, IRS (Aug. 6, 2024), <https://www.irs.gov/newsroom/multi-factor-authentication-key-protection-to-tax-professionals-security-arsenal-now-required>; *Multi-Factor Authentication*, PCI SECURITY STANDARDS COUNCIL (Feb. 2017), <https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf>; *A guide to the FTC Safeguards Rule's FTC MFA requirement*, IS DECISIONS (July 21, 2023), <https://www.isdecisions.com/en/blog/compliance/compliance-with-the-ftc-mfa-requirement>; *PCI DSS 4.0: New multi-factor authentication requirements*, ONESPAN (May 23, 2024), <https://www.onespan.com/blog/new-mfa-requirements-in-PCI-DSS-4.0>; *Multifactor Authentication Cheat Sheet*, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html (last visited Apr. 28, 2025).

⁷⁴ *Principal Cybersecurity - Encryption at Rest and Secrets Management*, AT&T, <https://web.archive.org/web/20241102115521/https://www.att.jobs/job/dallas/principal-cybersecurity-encryption-at-rest-and-secrets-management/117/71259367328> (archived Nov. 2, 2024).

⁷⁵ Chris Maes, *Improve your AWS security posture, Step 3: Encrypt AWS data in transit and at rest*, LEVELBLUE (Jan. 19, 2023), <https://levelblue.com/blogs/security-essentials/improve-your-aws-security-posture-step-3-encrypt-aws-data-in-transit-and-at-rest>.

⁷⁶ Anastasios Arampatzis, *What is data-centric security?*, LEVELBLUE (Dec. 13, 2023), <https://levelblue.com/blogs/security-essentials/what-is-data-centric-security>.

the data unencrypted and unprotected, allowing ShinyHunters to immediately exploit the stolen data without having to decrypt it.

169. Furthermore, AT&T's failure to encrypt the data enhanced exposure and risk of harm to AT&T-Direct Plaintiffs and Class Members when the cache of data was posted on the Dark Web granting easy access and misuse of the data.

170. Vulnerability scans of all systems, particularly those systems containing PII, should be done frequently. A vulnerability scan is an automated process used to identify security weaknesses or vulnerabilities in a computer system, network, application, or device. Organizations perform these scans regularly to detect and address potential threats before they can be exploited by attackers. Vulnerability scans are an essential part of proactive cybersecurity practices and play a crucial role in maintaining a secure IT environment. Readily available, intuitive, and easy-to-use specialized software tools are used to perform vulnerability scans. These tools examine the target system's configurations, files, software versions, and open network ports to identify potential security flaws. Common tools include Nessus, Qualys, and OpenVAS. After the scan, a report is generated detailing the identified vulnerabilities, their severity levels, and recommendations for remediation. This helps security teams prioritize and address the most critical vulnerabilities first. Vulnerability scans could have potentially detected malware that was used during the Data Breach.

171. Any organization that utilizes cloud storage or services should be focused on cloud security. Simply relying on the cloud vendor to meet all security needs is not recommended. There are specific standards and guidelines readily available to assist any organization in managing cloud security:

- i. ISO 27017 is guidance for cloud security. It applies the guidance of ISO 27002 to the cloud with seven additional controls.

- ii. ISO 27018 is closely related to ISO 27017. ISO 27018 defines privacy requirements in a cloud environment, particularly how the customer and cloud provider must protect PII.
- iii. NSA Cloud Security Strategies.⁷⁷
- iv. OWASP Cloud-Native Application Security Top 10.⁷⁸
- v. Checkpoint Security Top 15 Cloud Security Issues.⁷⁹
- vi. NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing.⁸⁰

172. Given that ShinyHunters frequently attacks cloud repositories, improved cloud security can mitigate attacks from this group, as well as other cyber threat groups. If ShinyHunters gained access to customer PII through AT&T's cloud storage, then the Data Breaches could have been prevented by following industry standards for cloud security.

⁷⁷ *NSA Releases Top Ten Cloud Security Mitigation Strategies*, NSA (Mar. 7, 2024), <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/>.

⁷⁸ *OWASP Cloud-Native Application Security Top 10*, OWASP FOUNDATION <https://owasp.org/www-project-cloud-native-application-security-top-10/> (last visited Apr. 28, 2025).

⁷⁹ *Top 15 Cloud Security Issues, Threats and Concerns*, CHECK POINT, <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/> (last visited Apr. 28, 2025).

⁸⁰ Wayne Jansen & Tim Grance, *NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing*, NIST (Dec. 2011), <https://csrc.nist.gov/pubs/sp/800/144/final>.

4. **AT&T Represents that It Has Cybersecurity Expertise, and It Should Have Been Well Equipped to Prevent a Data Breach**

173. AT&T has a cybersecurity division which offers cybersecurity services to other companies.⁸¹ AT&T specifically markets intrusion detection services,⁸² vulnerability assessment,⁸³ and even cybersecurity certifications.⁸⁴ This division was spun off into a separate entity called Level Blue⁸⁵ and has over 1,000 employees.⁸⁶

174. The Level Blue service touts a wide range of cybersecurity services:⁸⁷

Cyber Risk Advisory

Strategy and Roadmap Planning

Position yourself to deliver the advantages of digital transformation, manage related risks and help build customer trust

Risk and Compliance Assessment

Design a cybersecurity strategy that rationalizes your investments and streamlines operations

Security Program Remediation

⁸¹ LevelBlue, <https://cybersecurity.att.com/> (last visited Apr. 28, 2025).

⁸² *Intrusion detection system (IDS) software*, LEVELBLUE, <https://cybersecurity.att.com/solutions/intrusion-detection-system> (last visited Apr. 28, 2025).

⁸³ *Network vulnerability assessment*, LEVELBLUE, <https://cybersecurity.att.com/solutions/vulnerability-assessment-remediation> (last visited Apr. 28, 2025).

⁸⁴ *LevelBlue Certification*, LEVELBLUE, <https://cybersecurity.att.com/certification> (last visited Apr. 28, 2025).

⁸⁵ Robert Lemos, *AT&T Splits Cybersecurity Services Business, Launches LevelBlue*, DARK READING (May 6, 2024), <https://www.darkreading.com/cybersecurity-operations/att-splits-cybersecurity-services-business-launches-levelblue>.

⁸⁶ Steve McDowell, *AT&T Spins-Out Cybersecurity Business, LevelBlue*, FORBES (May 7, 2024), <https://www.forbes.com/sites/stevemcdowell/2024/05/07/att-spins-out-cybersecurity-business-levelblue/>.

⁸⁷ *Cybersecurity Consulting Services*, LEVELBLUE, <https://cybersecurity.att.com/consulting-services> (last visited Apr. 28, 2025).

Incorporate risk analytics for more informed decision making

IAM and Payment Security

Implement the right Identity and Access Management solution for your user authentication and privileges policies

Privacy and data governance and management

LevelBlue offers a suite of services—Privacy Program Strategy, Assessment, Design, and Implementation—demonstrating our dedication to helping organizations safeguard personal data and privacy. Our proactive approach guides clients through complex regulatory requirements, ensuring they stay ahead of industry-standard privacy frameworks and technological innovations.

Supply Chain Security

Extend advanced analytics across your entire supply chain—regardless of where it stretches

Cyber Operations

Network and Cloud Security

Take a holistic approach to securing digital and business transformation in the cloud

Cyber Security Operations Design (SOC) and Implementation

Develop and enhance cyber security operations through strategic design and implementation services

Cyber Transformation

Transform your existing traditional environment into a next-gen, application-aware highly-secure environment

Threat Detection and Response

Reduce, manage, and mitigate risks by enhancing your ability to detect and respond to threats in real time

Mobility/IoT and Endpoint Security Architecture and Design

Monitor and defend your endpoints from sophisticated threats, by detecting and responding autonomously at machine speed

Cybersecurity-as-a-Service (CaaS)

Vulnerability Threat and Fraud Management

Identify and address system vulnerabilities, to gain control and improve your risk posture

Security Awareness and Training

Help your employees understand and react appropriately to your organization's cyber risks

Third-party Risk and Compliance Management

Improve third-party cybersecurity governance and oversight using workflow automation and cyber risk scoring

Incident Readiness services

Get help from our cybersecurity consultants in understanding your strengths and identifying where you can close security gaps to improve your operational readiness.

Incident Response services

Have an experienced team of cybersecurity experts standing by to help you respond quickly and effectively in the event of a breach.

Trusted advisor-on-demand/virtual CISOaaS

Get the cybersecurity leadership you need—quickly and cost effectively

Security Orchestration Services

Enlist our efficient and effective project managers to help implement your cybersecurity programs with key stakeholders

175. Level Blue also touts that its services keep companies proactive, ahead of threats, and compliant with cybersecurity regulations and standards⁸⁸:

Stay Ahead of Threats

Reduce, manage, and mitigate risks by enhancing your ability to detect and respond to threats in real-time

⁸⁸ *Id.*

Maximize Resilience

Identify and address system vulnerabilities, gain control over your risk posture, and strengthen incident detection

Meet and Sustain Compliance

Let us help your organization comply with and manage industry regulations and standards

176. AT&T has sophisticated cybersecurity resources and expertise, which should have allowed it to recognize the well-known threat actor ShinyHunters's tactics and follow industry standard cybersecurity practices to prevent the Data Breach.

D. AT&T HAD A DUTY TO FOLLOW GUIDANCE AND INDUSTRY-STANDARD CYBERSECURITY PRACTICES

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

1. FCC's Consent Decrees

178. As described above, following AT&T's previous data breaches led to enforcement actions by the FCC resulting in two consent decrees that AT&T was legally obligated to implement and which are indicative of its issues effectively managing its cybersecurity.

179. Under the terms of the 2015 Consent Decree, AT&T agrees to pay a \$25 million civil penalty, and to implement a wide-ranging compliance plan, which includes the following key elements:

- Initial Risk Assessment: AT&T was required to conduct a comprehensive initial risk assessment to identify internal vulnerabilities, particularly those associated with unauthorized access to sensitive customer data (Customer Proprietary

Network Information, or CPNI). This assessment needed to evaluate risks posed by employees and third-party vendors.

- Regular Updates to the Risk Assessment: AT&T had to regularly review and update the risk assessment. While the 2015 Consent Decree did not explicitly prescribe a fixed schedule (*e.g.*, annual or biannual assessments), it stipulated that AT&T must continuously evaluate and address evolving risks as part of its ongoing compliance obligations.
- The risk assessments were required to examine: (i) Internal controls over employee and vendor access to customer data; (ii) The effectiveness of existing security policies and procedures; (iii) Areas of potential weakness in AT&T's broader information security framework; and (iv) Steps needed to mitigate any identified risks.
- Reporting Requirements: As part of the consent decree, AT&T was obligated to report its compliance efforts, including the results of risk assessments, to the FCC through periodic compliance reports.

180. In issuing the 2015 Consent Decree, the FCC stated that “[t]he Commission has made clear that it expects telecommunications carriers such as AT&T to take ‘every reasonable precaution’ to protect their customers’ data, and that it is committed to protecting the personal information of American consumers from misappropriation, breach, and unlawful disclosure.” 2015 Order. It is clear that when AT&T first learned of the AT&T-Direct Data Breach in 2021 and reviewed the dataset, that it failed to take “every reasonable precaution” in compliance with the FCC’s order to ensure that customer data was secure—otherwise the Data Breach could have been discovered years earlier.

181. Notably, the 2015 Consent Decree also required that AT&T take steps to ensure that its vendors are in compliance and safely handling customer data, and included that AT&T engage in “ongoing monitoring of Vendors’ compliance with their security obligations and implementing measures to sanction Vendors that fail to comply with their security obligations (*including, where appropriate, terminating AT&T’s relationship with such Vendors*).” 2015 Consent Decree at 7 (emphasis added).

182. Further highlighting AT&T’s continued and persistent cybersecurity deficiencies that existed in 2019, following a major breach in 2023 (described above) that exposed the personal information of approximately 9 million wireless customers, the FCC issued a new consent decree.

183. The FCC’s 2024 order expanded on the earlier mandate, revealing that despite previous corrective measures, AT&T’s data security practices remained insufficient. AT&T was required to overhaul its cybersecurity protocols, with a specific focus on securing its cloud infrastructure. AT&T had to implement stronger vendor oversight to address weaknesses in third-party data handling. Enhanced monitoring and detection systems were also required to identify and respond to potential threats in real-time, indicating that AT&T did not have sufficient monitoring and detection systems in place. Additionally, AT&T was ordered to provide detailed public disclosures about its data protection efforts and any breaches that occurred, along with enhanced customer remediation, including more robust credit monitoring services.

184. Even apart from the FCC’s consent decrees, AT&T was under a general obligation to act pursuant to the Communications Act of 1934 (“Communications Act”) as a telecommunications provider. Under the Communications Act, particularly sections 201(b) and 222(a), the Federal Communications Commission (“FCC”) requires carriers to safeguard PII and

Customer Proprietary Network Information (“CPNI”).⁸⁹ Section 201(b) establishes the general requirement that carriers operate in a “just and reasonable” manner, which informs the FCC’s enforcement of privacy protections.

185. The failure to reasonably secure customers’ PII “violates a carrier’s statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act.”⁹⁰ The FCC has made clear that it expects telecommunications carriers such as AT&T to take “every reasonable precaution” to protect their customers’ data, and that it is committed to protecting the personal information of American consumers from misappropriation, breach, and unlawful disclosure.⁹¹ In addition, the laws that require prompt disclosure of data breaches to law enforcement authorities, and subsequently to consumers, aid in the pursuit and apprehension of bad actors and provide valuable information that helps affected consumers be proactive in protecting themselves in the aftermath of a data breach.

2. FTC Guidance Regarding Safeguarding Customer Data

186. AT&T also failed to comply with FTC guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted by the FTC, failing to use reasonable

⁸⁹ The FCC previously defined “Personal Information” to mean either of the following: (1) an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver’s license number or other government-issued identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

⁹⁰ See Order, *In the Matter of AT&T Services, Inc.*, No. EB-TCD-14-00016243AT&T (F.C.C. Apr. 8, 2015) (“2015 Order”), <https://docs.fcc.gov/public/attachments/DA-15-399A1.pdf>.

⁹¹ *Id.*

measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

187. To that end, the FTC recommends the following practices:

- limiting access to customer information to employees who have a business reason to see it;
- keeping customer information in encrypted files to provide better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of compromise, such as unexpectedly large amounts of data being transmitted to unknown users; and
- monitoring activity logs for signs of unauthorized access to customer information.⁹²

188. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁹³

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

⁹² *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), <https://www.lb7.uscourts.gov/documents/20-0046.pdf>.

⁹³ *Start With Security*, FED. TRADE COMM'N (June 2025), <http://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

businesses.⁹⁴ The guidelines note that businesses should protect the personal customer information that they keep; properly delete PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

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

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

192. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

⁹⁴ *Protecting PII: A Guide for Business*, FED. TRADE COMM'N, http://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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

193. The FTC has also interpreted Section 5 of the FTC Act to apply to failures to appropriately store and maintain personal data.

3. SEC Reporting Requirements

194. As a public company, AT&T was required to disclose any data breach that was a material cybersecurity incident. This disclosure rule took effect on September 5, 2023.

195. Companies are required to disclose any material security incident and outline its nature, scope, the timing of the incident, and its likely impact. Companies have four business days after determining an incident is material to file a Form 8-K, Item 1.05. But, if the U.S. attorney general says immediate disclosure would create substantial national security or public safety risk, companies can delay disclosure. The SEC is also requiring companies to amend their initial 8-K filings to disclose incident information that was not previously determined or available.

196. Despite AT&T being aware of the AT&T-Direct Data Breach since 2021, AT&T failed to file or amend an 8-K filing to inform the public and shareholders of the Data Breach because a “reasonable investor” would consider this incident significant to AT&T and so it was therefore obligated to report it.

4. Industry Standard Reporting Requirements

197. There are a number of standards and guidelines for incident response and reporting. NIST 800-62 is one such standard.⁹⁵ That standard explains that an enterprise’s reporting protocols should, “at a minimum, [state] what must be reported to whom and at what times (e.g., initial

⁹⁵ Paul Cichonski *et al.*, *Computer Security Incident Handling Guide*, NIST (Aug. 2012), <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.

notification, regular status updates).” The following individuals and entities should be notified of a potential data breach:

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)
- Law enforcement (if appropriate)

198. Every state has a data breach notification law which requires companies to notify affected individuals promptly following their discovery of a data breach.⁹⁶

199. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 also created federal requirements for data breach reporting.⁹⁷

⁹⁶ *Data Breach Notification Laws by State*, IT GOVERNANCE (July 2018), <https://www.itgovernanceusa.com/data-breach-notification-laws>.

⁹⁷ *Cyber breach reporting to be required by law for better cyber defense*, PWC, <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html> (last visited Apr. 29, 2025).

200. In December 2023, the FCC expanded the scope of its data breach notification rules for telecommunications carriers and iVoIP providers to cover more categories of PII and methods of unauthorized access.⁹⁸

201. Various other reliable sources provide guidance on how to handle a breach, all of which include prompt notification of affected parties and law enforcement.⁹⁹

202. Because AT&T denied any breach had occurred, it did not adhere to its obligations to properly notify state and federal government agencies or individual victims. Failure to notify the public put customers at risk because they could not then take proper precautions to defend themselves against identity theft and fraud. And failure to provide timely notification to law enforcement substantially limits their ability to perform any adequate investigation.

203. Rather than follow industry standards, AT&T instead denied any breach had occurred for two years and seven months.

204. When AT&T finally acknowledged a breach had occurred, their public statements indicated it was a recent breach, when that is not accurate. This would have misled past and present

⁹⁸ Yaron Dori, Conor Kane & John Webster Leslie, *The FCC Expands Scope of Data Breach Notification Rules*, COVINGTON (Jan. 4, 2024), <https://www.insideprivacy.com/technology/the-fcc-expands-scope-of-data-breach-notification-rules/>.

⁹⁹ *Data Breach Response: A Guide for Business*, FTC (Feb. 2021), <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>; *Data Breach Reporting Requirements*, 47 CFR Part 64, Fed. Reg. (Feb. 12, 2024), <https://www.federalregister.gov/documents/2024/02/12/2024-01667/data-breach-reporting-requirements>; *Breach Notification Rule*, HHS, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (last updated July 26, 2013); Luke Irwin, *What Are Your Data Breach Notification Requirements?*, IT GOVERNANCE (Apr. 20, 2023), <https://www.itgovernanceusa.com/blog/when-should-an-organization-report-a-data-breach>; Robbie Araiza, *Data Breach Rules & Regulations: Who To Notify and How Long You Have To Do It*, DIGITAL GUARDIAN (Dec. 30, 2022), <https://www.digitalguardian.com/blog/data-breach-rules-regulations-who-notify-and-how-long-you-have-to-do-it>.

customers about whether their information is likely to have been exposed in the AT&T Direct Data Breach.

5. Industry Standards Regarding Network Security

205. AT&T also failed to comply with industry standards relating to data security. Various cybersecurity industry best practices have been published, are readily available, and should be consulted as a go-to source for an entity instituting, developing, maintaining, or enhancing its cybersecurity standards.

206. These practices include, across all industries encountering PII, education and appropriate access restriction for all personnel in regard to proper creation, collection, maintenance, and use of Protected Information; enforcing strong password and similar protections, including multi-factor authentication; applying multi-layer security measures (including firewalls, antivirus, and anti-malware software); monitoring for suspicious or irregular traffic to servers, credentials used to access servers, activity by known or unknown users, and server requests; implementing encryption to render data unreadable without proper authorization; ensuring security of cloud storage; and regular back up of data.

207. Additional cybersecurity best practices include, but are not limited to, installing appropriate malware detection software, monitoring and limiting network posts, securing web browsers and e-mail systems, configuring network infrastructure (like firewalls, switches, and routers), safeguarding physical security systems, training staff on key cybersecurity aspects, monitoring for vulnerability alerts, and promptly detecting and addressing vulnerability alerts before exploitation by cybercriminals.

208. The ISO 27001 standard focuses on establishing, implementing, maintaining, and continually improving an information security management system. Adopting ISO 27001 standards mitigates risk of unauthorized access and data breaches.¹⁰⁰

209. The SOC 2 standard is another widely recognized standard in the United States. SOC 2 compliance ensures that data is managed in a way that protects privacy and security, requiring regular audits and controls over data access.¹⁰¹

210. The National Institute of Standards and Technology (“NIST”) and the Center for Internet Security, Inc. (“CIS”)¹⁰² have established standards for reasonable cybersecurity readiness.

211. Recognizing that the national and economic security of the United States is dependent upon the reliable function of critical infrastructure, President Barack Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013.

¹⁰⁰ *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, ISO (2022), <https://www.iso.org/standard/27001>.

¹⁰¹ *2018 SOC 2® Description Criteria (With Revised Implementation Guidance – 2022)*, AICPA & CIMA (Oct. 1, 2023), <https://www.aicpa-cima.com/resources/download/get-description-criteria-for-your-organizations-soc-2-r-report>.

¹⁰² CIS is a community-driven nonprofit responsible for globally recognized best practices for securing IT systems and data, including a prescriptive, prioritized, and simplified set of best practices in cybersecurity (referred to as “CIS Controls”) and consensus-based prescriptive configuration recommendations of global cybersecurity experts (referred to as “CIS Benchmarks”). Per the CI website, the CIS Controls are a general set of recommended practices for securing a wide range of systems and devices, whereas CIS Benchmarks are guidelines for hardening specific operating systems, middleware, software applications, and network devices. The need for secure configurations is referenced throughout the CIS Controls. In fact, CIS Control 4 specifically recommends secure configurations for hardware and software on mobile devices, laptops, workstations, and servers. Both the CIS Controls and the CIS Benchmarks are developed by communities of experts using a consensus-based approach. *See CIS Critical Security Controls FAQ*, CENTER FOR INTERNET SECURITY, <https://www.cisecurity.org/controls/cis-controls-faq> (last visited Apr. 28, 2025).

Executive Order 13636 directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. Created through collaboration between industry and government, the voluntary framework promotes the protection of critical infrastructure, and provides standards, guidelines, tools, and technologies to protect information technology systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services.

212. Cybersecurity and Infrastructure Security Agency (“CISA”) guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;
- Employing 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

- Disabling 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.¹⁰³

213. 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.¹⁰⁴ Likewise, the principle of least privilege (POLP) should be applied to all systems so that users only have the access they need to perform their jobs.¹⁰⁵

214. Not only should AT&T have had measures in place to prevent compromise in the first place, AT&T should have also properly siloed their systems so that a bad actor would be unable to escalate privileges and move laterally through AT&T's systems. A data silo can occur when an organization manages data separately without maintaining a centralized system to share and access information.¹⁰⁶

215. Similarly, the lack of segmented systems, which are common to cloud-based servers, allowed the hacker to travel among AT&T's systems freely, compromising multiple

¹⁰³ *Ransomware Guide*, Multi-State Information Sharing & Analysis Center, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security, at 4 (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

¹⁰⁴ *Id.* at 5.

¹⁰⁵ *Id.* at 6.

¹⁰⁶ *Id.* at 7-8; see also Robert Wood, *Why Data Silos Create Cybersecurity Risks and How to Break Them Down*, ACCELERATION ECONOMY (Feb. 27, 2023), <https://accelerationeconomy.com/cybersecurity/why-data-silos-create-cybersecurity-risks-and-how-to-break-them-down/#>.

systems which AT&T was unable to recover, and ultimately resulting in the complete shutdown of AT&T's operations.

216. CISA guidance recommends that using a comprehensive network, in addition to network segregation, will help contain the impact of an intrusion and prevent or limit lateral movement on the part of malicious actors.¹⁰⁷

217. AT&T was aware of its obligations to protect its customers' PII before the Data Breaches, yet failed to take reasonable steps to protect its customers' PII from unauthorized access. In this case, AT&T was at all times fully aware of its obligation to protect the PII of its customers. AT&T was also aware of the significant repercussions if it failed to do so because AT&T collected PII from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

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

E. THE EFFECT OF THE AT&T DATA BREACHES ON PLAINTIFFS AND CLASS MEMBERS

219. AT&T's failure to keep Plaintiffs' and Class Members' PII secure has severe ongoing ramifications. Given the sensitive nature of the PII stolen in the AT&T-Direct Breach—including names, addresses, email addresses, phone numbers, dates of birth, account numbers, and social security numbers—which was bundled together and designated as AT&T customer information—hackers can commit identity theft, financial fraud, and other identity-related fraud

¹⁰⁷ *Id.*

against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face a present and also imminent and substantial risk of further injury, including identity theft and related cybercrimes, due to the AT&T-Direct and AT&T-Snowflake Data Breaches.

220. As a as a direct and proximate result of AT&T's known deficient data security and failure to protect Plaintiffs' and Class Members' PII, as well as AT&T's concealment of the same, Plaintiffs and other Class Members have suffered and will suffer injury.

221. Plaintiffs and Class Members are further subjected to the imminent threat of privacy violations and the continuous threat to their personal and financial security due to the immutable nature (e.g., names, social security numbers, etc.) of the PII at issue. This vulnerability stems directly from the initial unauthorized disclosure of their sensitive information, which put Plaintiffs' sensitive personal information in the hands of criminals, amplifying the severity and scope of the consequences of both the AT&T-Direct and AT&T-Snowflake Data Breaches.

222. Plaintiffs and Class Members, therefore, must incur the ongoing costs, both in terms of time and financial, to research their respective Data Breach(es), monitor their accounts for fraudulent activity, review unsolicited emails, answer unwanted phone calls, and to pay for those services that may limit or prevent such intrusions and harm to occur, or face an even more increased risk of identity theft. Indeed, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

223. Plaintiffs and Class Members have suffered a loss of the value of their PII. AT&T collects, retains, and uses Plaintiffs' and Class Members' PII to increase its profits through

predictive and other targeted marketing campaigns. Plaintiffs' and Class Members PII is not only valuable to AT&T, as Plaintiffs and Class Members also place value on their PII based on their understanding that their PII is a financial asset to companies that collect it.¹⁰⁸ Similarly, Plaintiffs and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiffs' and Class Members' PII that was permitted without authorization by AT&T. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

224. In addition to the actual, present, concrete, and current injuries described above because of AT&T's actions and omissions, Plaintiffs and Class Members have suffered, and will continue to suffer perpetual emotional distress, worry, and other emotional or psychological harm, as well as the well-founded fear that additional, realistic, objectively reasonable, threatened, impending, sufficiently imminent harm in the form of identity theft or fraud will occur in the future.

225. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."¹⁰⁹ Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiffs will therefore need to spend time and

¹⁰⁸ See, e.g., *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers*, PONEMON INSTITUTE, LLC (Mar. 2015), <https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html> (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security Number at \$55.70).

¹⁰⁹ *GAO-07-737, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 4, 2007), <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm>.

money to continuously monitor their accounts for years to ensure their PII obtained in the Data Breaches is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breaches. In other words, Plaintiffs have been harmed by the value of identity protection services they must purchase now, and in the future, to ameliorate the risk of harm they face due to the Data Breaches.

226. As described herein for each individual Plaintiff, Plaintiffs have invested, and will continue indefinitely to invest, time and money into precautionary measures that *could*, but may not successfully, mitigate the potential misuse of their data compromised in the Data Breaches.

227. The presence of Plaintiffs' PII on the Dark Web as acknowledged by AT&T and as the result of AT&T's cybersecurity deficiencies and failure to protect its customers' PII, significantly increases the risk of further substantial damage to Plaintiffs and the Class, including, but not limited to, monetary and identity theft.

228. Moreover, Plaintiffs and Class Members value the privacy of the information they provided to AT&T and expected AT&T to allocate sufficient resources to ensure it is adequately protected. Customers would not have done business with AT&T, provided their PII and payment card information, or paid the same prices for AT&T goods and services had they known AT&T did not implement reasonable security measures to protect their PII. As a result, Plaintiffs and Class Members did not receive the benefit of their bargain with AT&T because they paid a value for services that they reasonably expected but did not receive.

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

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

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

231. To date, Defendants have done nothing to provide Plaintiffs and the Class Members with adequate relief for the damages they have suffered as a result of the Data Breaches.

232. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII and PHI, which remains in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not

accessible online, that access to such data is password-protected, and that such data is properly encrypted.

233. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII, which contains the most intimate details about a person's life, may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

1. Plaintiffs' PII Has Measurable Intrinsic Value

234. Plaintiffs and Class Members entrusted Defendants with sensitive and valuable PII, including but not limited to full names, SSNs, addresses, birthdates, and passcodes. This data has actual, measurable value in today's digital economy.

235. The compromised PII is of particular economic value because it cannot be easily changed. A compromised password can be reset. A stolen Social Security number or birthdate cannot. It is immutable. This permanence renders the information more useful—and therefore more valuable—to identity thieves and data brokers.

236. Defendants themselves recognize the importance and value of safeguarding PII. They offer paid services—such as scam protection and identity theft monitoring—for fees ranging from \$3.99 to \$19.99 per month.¹¹⁰

237. As a result of Defendants' failure to adequately safeguard the PII of students and teachers, Plaintiffs and Class Members seek compensatory damages for the measurable value of their compromised data, the cost of future protective measures, time spent remedying exposure, and non-economic damages arising from the violation of privacy rights.

¹¹⁰ AT&T ActiveArmor Pricing, att.com (last accessed: Apr. 14, 2025).

2. Privacy Can Also Be Measure By Cost Paid For It

238. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Prey, a company that develops device tracking and recovery software, stolen PII can be worth up to \$2,000.00 depending on the type of information obtained.¹¹¹

239. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII, particularly social security numbers, to open new bank accounts, take out loans, start new utility accounts, and incur charges and credit in a person's name.^{112, 113}

240. There are time lags between when PII is stolen, when it is used, and when a person discovers it has been used. On average, it takes about three months for consumers to discover that their identity has been stolen and used, but it takes some people up to three years to learn that information.¹¹⁴

241. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

¹¹¹ Juan Hernandez, *The Lifecycle of Stolen Credentials on the Dark Web*, PREY (Feb. 26, 2024), <https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web>.

¹¹² *What to Know About Identity Theft*, FED. TRADE COMM'N (Apr. 2021), <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft>.

¹¹³ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 12 C.F.R. §1022.3(h). The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 12 C.F.R. §1022.3(g).

¹¹⁴ John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS & INFORMATICS, 12 (2019), <https://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf> (last accessed Mar. 17, 2025).

242. One such example of criminals using PII for profit is the development of “Fullz” packages, or dossiers on individuals.¹¹⁵ The development of Fullz packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. Importantly, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members.

243. According to the U.S. Federal Bureau of Investigation (“FBI”), in 2023, Internet-enabled crimes reached their highest number of complaints and dollar losses, resulting in more than \$12.5 billion in losses to individuals and business victims.¹¹⁶

¹¹⁵ “Fullz” is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information one has on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KREBS ON SEC. (Sept. 18, 2014), <https://krebsonsecurity.com/tag/fullz/>.

¹¹⁶ 2023 *Internet Crime Report*, FBI INTERNET CRIME COMPLAINT CTR. (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

244. The FBI states that “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”¹¹⁷ Here, AT&T did not rapidly report to Plaintiffs and Class Members that their PII had been stolen, but rather denied the AT&T-Direct Data Breach for years.

245. Experian, one of the largest credit reporting companies in the world, warns consumers that “[i]dentity thieves can profit off your personal information” by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.¹¹⁸

246. In addition to out-of-pocket expenses that can exceed thousands of dollars, and the emotional toll identity theft can take, some victims have to spend considerable time repairing the damage caused by the theft of their PII and PHI.

247. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.¹¹⁹ Victims of new account identity theft will likely have to spend time correcting fraudulent

¹¹⁷ *2019 Internet Crime Report Released*, FBI INTERNET CRIME COMPLAINT CTR. (Feb. 11, 2020), <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=Rapid%20reporting%20can%20help%20law,to%20build%20on%20its%20success.>

¹¹⁸ Louis DeNicola, *What Can Identity Thieves Do With Your Personal Info and How Can You Protect Yourself?* EXPERIAN (May 21, 2023), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

¹¹⁹ *2023 Consumer Impact Report*, IDENTITY THEFT RES. CTR. (Aug. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.

information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank and credit accounts, open new ones, and dispute charges with creditors.

248. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated, “[m]ost consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”¹²⁰

249. As a result of the AT&T Data Breaches, Plaintiffs’ and Class Members’ PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, their PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

250. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.¹²¹ According to the FTC, data security requires: (a) encrypting information stored on computer networks; (b) retaining payment card information only as long as necessary; (c) properly disposing of personal information that is no longer needed; (d) limiting administrative access to business systems; (e) using industry-tested and accepted methods

¹²⁰ *Commissioner Pamela Jones Harbour, Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM’N, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

¹²¹ *Start with Security: A Guide for Business*, FED. TRADE COMM’N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

for securing data; (f) monitoring activity on networks to uncover unapproved activity; (g) verifying that privacy and security features function properly; (h) testing for common vulnerabilities; and (i) updating and patching third-party software.¹²²

251. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.¹²³ The FTC treats 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(a) of the FTC Act.

252. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive consumer data. *See In re Lookout Servs., Inc.*, 151 F.T.C. 532, 535 (June 15, 2011) (the defendant “allowed users to bypass authentication procedures” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs”); *In re DSW, Inc.*, 2006 WL 6679055, at *2 (FTC Mar. 7, 2006) (the defendant “failed to employ sufficient measures to detect unauthorized access”); *In re TJX Cos., Inc.*, 2008 WL 3150421, at *2, (FTC Jul. 29, 2008) (“[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]” and “failed to employ sufficient measures to detect and prevent unauthorized access to computer networks”); *In re Dave & Buster's Inc.*, No. C-4291 (FTC May

¹²² *Id.*

¹²³ *Taking Charge: What to Do if Your Identity is Stolen*, U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS (Jan. 2012), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen>.

20, 2010) (the defendant “failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization” and “failed to use readily available security measures to limit access between in-store networks”). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

253. AT&T failed to adequately protect Plaintiffs’ and Class Members’ PII and allowed criminals unfettered access to this sensitive data to use in the conduct of criminal activity. Specifically, AT&T failed to adequately protect Plaintiffs’ and Class Members’ PII from people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII and PHI.

254. AT&T’s failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiffs and potentially millions of Class Members from unscrupulous operators, con artists, and outright criminals.

255. AT&T’s failure to properly and timely notify Plaintiffs and Class Members of the Data Breaches exacerbated Plaintiffs’ and Class Members’ injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ALLEGATIONS

256. Plaintiffs bring this class action individually on behalf of themselves and on behalf of all similarly situated persons of the following nationwide classes and AT&T-Direct nationwide subclasses (together, the “Classes”) pursuant to Federal Rule of Civil Procedure 23. As described below, this action satisfies the numerosity, commonality, typicality, adequacy, predominance, and

superiority requirements of Rule 23(a), 23(b)(2), and 23(b)(3) (as well as the requirements for certification of one or more issue classes under Rule 23(c)(4)). Accordingly, Plaintiffs seek certification of the following Classes:

NATIONWIDE CLASSES

257. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiffs seek certification of the following nationwide classes (“Nationwide Classes”):

- a. **AT&T-Direct Class:** All living persons in the United States whose information may have been accessible in the cybersecurity incident announced by AT&T on or about March 30, 2024, and includes some combination of names, addresses, telephone numbers, email addresses, dates of birth, account passcodes, billing account numbers, and Social Security numbers.
- b. **AT&T-Snowflake Class:** All AT&T Account Owners or Line or End Users whose telephone numbers, along with the telephone numbers with which those customers interacted, counts of those interactions, aggregate call durations for a day or month, and for a small subset of individuals, one or more cell site identification numbers associated with the interactions, may have been accessible and were involved in the incident announced by AT&T on or about July 12, 2024.

258. The Nationwide Classes assert claims against AT&T for violations of the Communications Act, 47 U.S.C. § 201, *et seq.* (Count 1), breach of implied contract (Count 4); negligence (Count 5), and declaratory judgment and injunctive relief (Count 6).

AT&T-DIRECT NATIONWIDE SUBCLASSES

SATELLITE ACT SUBCLASS

259. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide Subclass (“Satellite Act Subclass”):

All natural persons residing in the United States who were subscribers to AT&T’s services and whose personally identifiable information was collected or maintained in AT&T’s capacity as a satellite carrier, including, but not limited, to DirecTV subscribers, and whose personally identifiable information was included in the

data set released on the dark web, as referenced in AT&T's March 30, 2024, announcement of a data breach.

260. The Satellite Act Subclass asserts claims against AT&T for violations of the Satellite Act pursuant to 47 U.S.C. § 338(i)(7) (Count 2).

CABLE ACT SUBCLASS

261. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide Subclass ("Cable Act Subclass"):

All natural persons residing in the United States who were subscribers to AT&T's services, whose personally identifiable Information was collected or maintained in AT&T's capacity as a cable provider, including, but not limited to, U-Verse subscribers, and whose personally identifiable information was included in the data set released on the dark web, as referenced in AT&T's March 30, 2024, announcement of a data breach.

262. The Cable Act Subclass asserts claims against AT&T for violations of the Cable Act pursuant to 47 U.S.C. § 551(f) (Count 3).

263. Excluded from the Nationwide Classes and Nationwide Subclasses are AT&T, any entity in which AT&T has a controlling interest, and AT&T's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Classes and the Nationwide Subclasses are any judicial officer presiding over this matter, Members of their immediate family, and Members of their judicial staff.

264. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The Members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, AT&T has acknowledged that the PII of millions of individuals has been compromised. The names and addresses of those individuals are available from AT&T's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved

notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Nationwide Subclass, making joinder of all Subclass Members impracticable.

265. Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3). As to each Class and Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. These common questions include:

- i. Whether and to what extent AT&T had a duty to protect the confidentiality of the PII of its customers and former customers;
- ii. Whether AT&T failed to take reasonable and prudent security measures to ensure its systems were protected;
- iii. Whether AT&T failed to use reasonably available information to monitor its systems and prevent the Data Breaches from happening;
- iv. Whether AT&T knew or should have known that its computer and data storage systems were vulnerable to compromise;
- v. Whether AT&T was negligent in failing to implement reasonable and adequate security procedures and practices;
- vi. Whether AT&T's security measures to protect its systems were reasonable in light of applicable legal and regulatory requirements and industry standards;
- vii. Whether AT&T's data security practices were unjust or unreasonable under the Communications Act, 47 U.S.C. § 201(b);
- viii. Whether AT&T complied with federal law and took such actions as were necessary to prevent unauthorized access to its customers' PII by persons other than the customer and AT&T, as required by the Cable Act and Satellite Act;

ix. Whether AT&T had any contractual obligations to provide for the security of its customers' PII;

x. Whether AT&T has complied with any contractual obligations to protect its customers' PII;

xi. Whether AT&T failed to notify Plaintiffs and Class Members as soon as practicable and without delay after each of the Data Breaches was discovered;

xii. Whether AT&T's conduct resulted in or was the proximate cause of the loss of the PII of Plaintiffs and Class Members;

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

xiv. Whether AT&T should retain the money paid by Plaintiffs and Class Members to protect their PII as well as the profits AT&T generated using Plaintiffs' and Class Members' PII;

xv. Whether AT&T should retain Plaintiffs' and Class Members' valuable PII;;
and

xvi. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

266. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to each Class and Subclass, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and harmed in the same way. Plaintiffs' PII was in AT&T's possession at the time of the Data Breaches and was compromised as a result of the Data Breaches. Plaintiffs' damages and injuries are akin to those of other Class Members, and Plaintiffs seek relief consistent with the relief of the Class.

267. Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).

Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are Members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

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

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

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

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

272. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CHOICE OF LAW

273. The State of Texas has a significant interest in regulating the conduct of businesses operating within its borders. Texas, which seeks to protect the rights and interests of Texas and all residents and citizens of the United States against a company headquartered and doing business in Texas, has a greater interest in the nationwide claims of Plaintiffs and Nationwide Class Members than any other state and is most intimately concerned with the claims and outcome of this litigation.

274. The principal place of business of AT&T, located at 208 South Akard Street, Dallas, Texas 75201—also known as One AT&T Plaza—is the “nerve center” of its business

activities—the place where its high-level officers direct, control, and coordinate the corporation’s activities, including its data security functions and major policy, financial, and legal decisions.

275. AT&T’s response to the data breaches at issue here, and corporate decisions surrounding such response, were made from and in Texas, including the following allegations central to Texas as described in a declaration by Paula Phillips, a Direct—Legal Administrator of AT&T Services, Inc. that has been in the Legal Department for the AT&T family of companies since 1991:

a. AT&T’s cybersecurity incident response was directed from Dallas, Texas. *In re: AT&T Data Breach Litigation*, MDL No. 3114, Docket No. 93-1 at 2-3 (J.P.M.L. May 2, 2024);

b. Key leadership for AT&T’s wireless business is and was located in Dallas, including “marketing, finance, sales and distribution, the organization the builds the wireless network, and customer operations, which has certain incident response and breach remediation responsibilities” (*Id.*);

c. AT&T’s Chief Information Security Officer is based in Dallas, Texas (*Id.*);

d. AT&T’s Chief Technology Officer, Jeremy Legg, spends “considerable time (usually every other week) at AT&T’s Dallas offices where most of his direct reports sit” (*Id.*); and

e. AT&T’s Chief Data Officer, Andy Markus, spends “significant time at AT&T’s Dallas offices. Mr. Markus has twice as many employees in his organization working in Texas (approximately 37%)” than in any other part of the country—with Georgia and New Jersey having approximately 19% each and with the remaining 25% spread across the country (*Id.*).

276. AT&T's breaches of duty to Plaintiffs and Nationwide Class Members emanated from Texas.

277. Application of Texas law to the Nationwide Class with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because Texas has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

278. Under Texas' choice of law principles, which are applicable to this action, the common law of Texas applies to the nationwide common law claims of all Nationwide Class Members. Courts sitting in diversity have similarly applied the laws of the state of residence for a corporation when analyzing choice of law questions in the data breach context. *See e.g., In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1312 (N.D. Ga. 2019).

COUNT 1
VIOLATION OF THE COMMUNICATIONS ACT
47 U.S.C. § 201, *et seq.*
(On Behalf of the Nationwide Classes against all Defendants)

279. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 278 and incorporate the same as if set forth herein.

280. Plaintiffs bring this Count on behalf of the Nationwide Class under Section 207 against all Defendants to recover damages resulting from AT&T's violations of Sections 201(b) and 222(a) of the Communications Act. *See* 47 U.S.C. § 201, *et seq.* *See also, Global Crossing Telecomm., Inc. v. Metrophones Telecomm. Inc.*, 550 U.S. 45 (2007). AT&T is a telecommunications carrier subject to the Communications Act and its enabling regulations. 47 U.S.C. § 153(11).

281. Pursuant to Section 201(b), “[a]ll charges, practices, classifications, and regulations [of a common carrier] for and in connection with [interstate or foreign] communication service [by wire or radio] *shall be just and reasonable*, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful.” 47 U.S.C. § 201(b) (emphasis added).

282. Section 222, entitled “Privacy of customer information,” requires telecommunications carriers to “protect the confidentiality of *proprietary information of*, and relating to, other telecommunication carriers, equipment manufacturers, and *customers*” 47 U.S.C. § 222(a) (emphasis added). “In the context of Section 222, it is clear that Congress used the term ‘proprietary information’ broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy.” *In re TerraCom, Inc.* 29 FCC Rcd. 13325, ¶ 14 (2014). The FCC has consistently interpreted “proprietary information” in Section 222(a) as “clearly encompassing private information that customers have an interest in protecting from public exposure,” such that telecommunication carriers are required “to protect sensitive private information.” *Id.* (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927, 6959, ¶ 64 (2007)).

283. The FCC has consistently concluded that the Communications Act requires telecommunication carriers to “take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.” *See In re TerraCom*, 29 FCC Rcd. 13325, ¶ 12 (quoting 22 FCC Rcd 6927, 6959, ¶ 64 (2007)).

284. The FCC has consistently concluded that a telecommunication carrier’s “failure to reasonably secure customers’ proprietary information violates a carrier’s statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act.” *In re AT&T Services, Inc.*, 30 FCC Rcd. 2808, 2808 (2015); *see also In re TerraCom, Inc.*, 29 FCC Rcd. 13325, ¶ 12 (2014) (“By failing to employ reasonable data security practices to protect consumers’ PI, the Companies also engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act.”).

285. Further, the FCC has historically concluded that a telecommunication carrier’s failure to notify its customers of a potential data breach is an unjust and unreasonable practice in violation of Section 201(b) because the failure deprives the customers of an opportunity to take steps to protect their personal information from misappropriation by third parties. *See In re TerraCom*, 29 FCC Rcd. 13325, ¶ 12.

286. Defendants’ business practices concerning Plaintiffs’ and Nationwide Class Members’ PII were unjust and unreasonable and violated Sections 201(b) and 222(a) of the Communications Act in that Defendants:

- a. Failed to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Nationwide Members’ PII, which was a direct and proximate cause of the Data Breaches;
- b. Failed to implement a reasonable Data Retention and Deletion Policy;
- c. Failed to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breaches;

d. Failed to exercise due diligence in vetting, selecting, and monitoring the activities of third-party vendors who were entrusted with handling and storing Plaintiffs' and Nationwide Members' PII, thereby exposing that PII to unreasonable security and privacy risks, which was a direct and proximate cause of the Data Breaches;

e. Failed to adequately and timely respond to suspicious or anomalous account activity and to otherwise detect and prevent the exfiltration of Plaintiffs' and Nationwide Members' PII, which was a direct and proximate cause of the Data Breaches;

f. Failed to implement reasonable administrative, technical, and physical safeguards to protect the security and confidentiality of Plaintiffs' and Nationwide Members' PII, which was a direct and proximate cause of the Data Breaches;

g. Misrepresented that it would protect the privacy and confidentiality of Plaintiffs' and Nationwide Class Members' PII, including by implementing and maintaining reasonable security measures;

h. Misrepresented its compliance with common law, statutory, and regulatory duties pertaining to the security and privacy of Plaintiffs' and Nationwide Class Members' PII;

i. Omitted, suppressed, and concealed the material fact that Plaintiffs' and Nationwide Class Members' PII had been exposed on the dark web; and

j. Failed to give timely, adequate, and reasonable notice to Plaintiffs and Nationwide Class Members of the AT&T-Direct Data Breach, thereby depriving and impairing the opportunity to take steps to protect their personal information from misappropriation by third parties; and

k. Failed to act in a just and reasonable manner upon learning its customers' data was available for sale on the Dark Web.

287. Pursuant to 47 USC § 217, “In construing and enforcing the provisions of this chapter, the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person.”

288. Defendants’ violations of Section 201(b) and Section 222(a) of the Act have caused substantial monetary damage to Plaintiffs and Nationwide Class Members, in such amounts to be proven at trial, together with such additional amounts as may accrue to the date of trial.

289. Section 206 of the Communications Act states that if “any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation” 47 U.S.C. § 206, Defendants are accordingly liable to Plaintiffs and Nationwide Class Members for the full amount of damages they sustained in consequence of AT&T’s violations of Sections 201(b) and 222(a) of the Communications Act. Defendants are also liable for Plaintiffs’ reasonable attorneys’ fees pursuant to 47 U.S.C. § 206.

COUNT 2
VIOLATION OF THE SATELLITE HOME VIEWER EXTENSION
AND REAUTHORIZATION ACT
47 U.S.C. § 338(i)
(On Behalf of the AT&T-Direct Nationwide Subclass against the AT&T-Direct Defendants)

290. AT&T-Direct Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 278 and incorporate the same as if set forth herein.

291. AT&T-Direct Plaintiffs bring this Count on behalf of the Satellite Act Subclass against the AT&T-Direct Defendants to recover their actual damages sustained and the liquidated

damages warranted as a consequence of the AT&T-Direct Defendants' violations of Section 338(i) of Title 47, *i.e.*, the "Satellite Act," particularly Section 338(i)(4)(A). *See* 47 U.S.C. § 338(i)(7). This statute is entitled "[p]rivacy rights of satellite subscribers" and governs the use, disclosure, and retention of "personally identifiable information" collected by a "satellite carrier" concerning the "subscribers" of a satellite service or "other service" provided by the satellite carrier, with those terms defined as set forth below. *See* 47 U.S.C. § 338(i).

292. The Satellite Act defines "personally identifiable information" ("PII") broadly, excluding only customer-related information that any record of aggregate data which does not identify particular persons." 47 U.S.C. § 338(i)(2)(A). The information contained in the subject Data Breach enabled the theft of specific individuals' identities and thus constituted PII as that term is defined by Section 338(i).

293. Second, the Satellite Act protects AT&T-Direct Plaintiffs and Nationwide Subclass Members who were subscribers to either satellite service or "other service" provided by a satellite carrier, with the latter term defined as including "any wire or radio communications service provided using any of the facilities of a satellite carrier that are used in the provision of satellite service." 47 U.S.C. § 338(i)(2)(B).

294. The AT&T-Direct Defendants are subject to the Satellite Act as a "satellite carrier" which expansively includes "in addition to persons within the definition of satellite carrier, any person who (i) is owned or controlled by, or under common ownership or control with, a satellite carrier; and (ii) provides any wire or radio communications service." *See* 47 U.S.C. § 338(i)(2)(C). At all relevant times herein, DirecTV has been a satellite carrier as that term is defined in the Satellite Act. 47 U.S.C. § 338(k)(7); 17 U.S.C. § 119(d)(6). As of July 24, 2015, and at all relevant

times thereafter, DirecTV was a “wholly-owned subsidiary” of AT&T¹²⁴ “under common ownership or control with AT&T,” such that AT&T was a satellite carrier under the Satellite Act. Subsidiaries and affiliated entities of AT&T providing other wire or radio communications services “using any of the facilities of a satellite carrier that are used in the provision of satellite service” are thus also subject to the Satellite Act, and the Satellite Act Subclass includes subscribers to these “other services” as well. *See* H. Rep. No. 102-628, 106–07 (1992) (discussing the intent of these definitions in the Cable Act); H.R. Rep. No. 108-634, at 19 (2004) (Section 338(i) intended to impose the same privacy obligations on satellite carriers as cable operators).

295. Under the Satellite Act, with exceptions that are not relevant here, a satellite carrier “shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or satellite carrier.” *See* 47 U.S.C. § 338(i)(4)(A).

296. The AT&T-Direct Defendants manifestly failed to “take such actions as [were] necessary” to prevent unauthorized access to PII concerning its subscribers, as evidenced by the publication of that PII on the Dark Web without the subscribers’ consent, and AT&T is strictly liable for that failure.

297. Further, the failure of the AT&T-Direct Defendants to prevent unauthorized access to subscribers’ PII also violated Section 338(i)(4)(A) of the Satellite Act in that AT&T:

¹²⁴ United States Securities and Exchange Commission (Form 15) (Nov. 9, 2015), www.sec.gov/Archives/edgar/data/1465112/000110465915077011/a15-22608_11512b.htm

a. Failed to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failed to implement a reasonable Data Retention and Deletion Policy;

c. Failed to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

d. Failed to exercise due diligence in vetting, selecting, and monitoring the activities of third-party vendors who were entrusted with handling and storing subscribers' PII, thereby exposing that PII to unreasonable security and privacy risks, which was a direct and proximate cause of the Data Breach;

e. Failed to adequately and timely respond to suspicious or anomalous account activity and to otherwise detect and prevent the exfiltration of subscribers' PII, which was a direct and proximate cause of the Data Breach; and

f. Failed to implement reasonable administrative, technical, and physical safeguards and security measures to protect the security and confidentiality of subscribers' PII, which was a direct and proximate cause of the Data Breach.

298. "Any person aggrieved by any act of a satellite carrier in violation of this section may bring a civil action in a United States district court." 47 U.S.C. § 338(i)(7). Plaintiffs and Subclass Members are aggrieved by AT&T's violations of Section 338(i)(4)(A), which directly and proximately caused their PII to be accessed without authorization by criminal elements and disbursed on the Dark Web, in violation of the privacy rights expressly recognized by the Satellite

Act. These violations of the Satellite Act have also caused substantial monetary damage to Plaintiffs and the Satellite Act Subclass, in such amounts to be proven at trial, together with such additional amounts as may accrue to the date of trial.

299. Under 47 U.S.C. § 338(i)(7)(A), the AT&T-Direct Defendants are liable to Plaintiffs and Subclass Members for actual damages sustained by Plaintiffs and Subclass Members in consequence of AT&T's violations of Section 338(i), but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher.

300. The AT&T-Direct Defendants are also liable for AT&T-Direct Plaintiffs' reasonable attorneys' fees and other litigation costs reasonably incurred pursuant to 47 U.S.C. § 338(i)(7)(C).

COUNT 3
VIOLATION OF THE CABLE TELEVISION CONSUMER
PROTECTION AND COMPETITION ACT
47 U.S.C. § 551

(On Behalf of the AT&T-Direct Nationwide Subclass against the AT&T-Direct Defendants)

301. AT&T-Direct Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 278 and incorporate the same as if set forth herein.

302. AT&T-Direct Plaintiffs bring this Count on behalf of the Cable Act Subclass to recover their actual damages sustained and the liquidated damages warranted as a consequence of AT&T-Direct Defendants' violations of Section 551 of Title 47, *i.e.*, the "Cable Act," particularly Section 551(c)(1). *See* 47 U.S.C. § 551(f). This statute is entitled "[p]rotection of subscriber privacy" and governs the use, disclosure, and retention of "personally identifiable information" collected by a "cable operator" concerning the subscribers of a "cable service" or "other service" provided by the cable operator, with those terms defined as set forth below. *See* 47 U.S.C. § 551.

303. The Cable Act defines “personally identifiable information” (“PII”) broadly, excluding only customer-related information that is “any record of aggregate data which does not identify particular persons.” *See* 47 U.S.C. § 551(a)(2)(A). The information contained in the subject Data Breach enabled the theft of specific individuals’ identities and thus constituted PII as Section 551 defines that term.

304. The Cable Act protects AT&T-Direct Plaintiffs and Nationwide Subclass Members who were of subscribers to either “cable service” or “other service” provided by a cable operator, with the latter term defined as including “any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service.” 47 U.S.C. § 551(a)(2)(B). “This specific definition of ‘other service’ plainly includes internet service transmitted via a cable system.” *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 157 F. Supp. 2d 286, 291 (S.D.N.Y. 2001).

305. At the time of the AT&T-Direct Data Breach, Time Warner and HBO were AT&T companies, later spun off in 2022.

306. AT&T-Direct Defendants are subject to the Cable Act as “cable operator[s]” which expansively includes, “in addition to persons within the definition of cable operator in [47 U.S.C. § 522(5)], any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.” 47 U.S.C. § 551(a)(2)(C). At all relevant times herein, AT&T’s provision of U-Verse services thus rendered it a cable operator as Section 551 defines that term, such that AT&T’s use, disclosure, and retention of the PII of its U-Verse subscribers was subject to Section 551

307. In addition, at the time of the AT&T-Direct Data Breach, Time Warner Cable, Inc. was a subsidiary of AT&T, and remains one of the largest cable providers in the United States.

308. As Congress explained when it enacted the Cable Television Consumer Protection and Competition Act of 1992, these expanded definitions were added to the Cable Act:

... to ensure that affiliated entities of the cable operator were included so that such entities could not avoid the privacy provisions merely because they were not directly offering cable service. For example, a cable operator could set up a separate subsidiary to offer radio communications service, or a cable operator could be a subsidiary of, or affiliated with, an entity offering wire or radio communications services. The Committee finds that such subsidiary or entity offering wire or radio communications services should adhere to the privacy provisions embodied in the Act and thus “cable operator” was defined for the purposes of this section of the Act to include any such person affiliated with the cable operator.

H. Rep. No. 102-628, 106–07 (1992). In light of this guidance, subsidiaries and affiliated entities of AT&T providing other wire or radio communications services “using any of the facilities of a cable operator that are used in the provision of cable service” are also subject to the Cable Act, and the Nationwide Cable Act Subclass includes subscribers to these “other services” as well.

309. Under the Cable Act, with exceptions that are not relevant here, a cable operator “shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.” *See* 47 U.S.C. § 551(c)(1).

310. Under Section 551 of the Cable Act, the AT&T-Direct Defendants were required to follow provisions for subscriber privacy protection, and implement policies to effectuate this legal obligation.

311. The Cable Act requires are required to clearly inform subscribers—both when they start service and at least once a year thereafter—about the PII they collect, how they use it, and with whom they may share it. 47 U.S.C. § 551. They must obtain prior written or electronic consent before collecting personal information through the cable system, except when it’s necessary to

provide services or prevent unauthorized access. *Id.* Disclosure of personal information without the subscriber's consent is prohibited unless it's essential for service provision, legitimate business activities, or mandated by a court order (in which case the subscriber must be notified). *Id.* Furthermore, cable operators are obligated to destroy personal information when it's no longer needed for its original purpose and there are no pending requests or court orders for access to that information. *Id.*

312. AT&T failed to destroy personal information for its former customers which constitute a majority of Class Members. This is in violation of the Cable Act as information provided to Time Warner, and now in AT&T's possession, would no longer be needed for its original purpose.

313. AT&T manifestly failed to "take such actions as [were] necessary" to prevent unauthorized access to PII concerning its subscribers, as evidenced by the publication of that PII on the Dark Web without the subscribers' consent, and AT&T is strictly liable for that failure.

314. Further, AT&T's failure to prevent unauthorized access to subscribers' PII also violated Section 551(c)(1) of the Cable Act in that AT&T-Direct Defendants:

- a. Failed to implement and maintain reasonable security and privacy measures to protect AT&T-Direct Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breaches;
- b. Failed to implement a reasonable Data Retention and Deletion Policy;
- c. Failed to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breaches;

d. Failed to exercise due diligence in vetting, selecting, and monitoring the activities of third-party vendors who were entrusted with handling and storing subscribers' PII, thereby exposing that PII to unreasonable security and privacy risks, which was a direct and proximate cause of the Data Breaches;

e. Failed to adequately and timely respond to suspicious or anomalous account activity and to otherwise detect and prevent the exfiltration of subscribers' PII, which was a direct and proximate cause of the Data Breaches; and

f. Failed to implement reasonable administrative, technical, and physical safeguards and security measures to protect the security and confidentiality of subscribers' PII, which was a direct and proximate cause of the Data Breaches.

315. "Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court." 47 U.S.C. § 551(f). Plaintiffs and Subclass Members are aggrieved by AT&T-Direct Defendants' violations of Section 551(c)(1), which directly and proximately caused their PII to be accessed without authorization by criminal elements and disbursed on the Dark Web, in violation of the privacy rights expressly recognized by the Cable Act. These violations of the Cable Act have also caused substantial monetary damage to AT&T-Direct Plaintiffs and the Cable Act Subclass, in such amounts to be proven at trial, together with such additional amounts as may accrue to the date of trial.

316. Under 47 U.S.C. § 551(f)(2)(A), Defendants are liable to AT&T-Direct Plaintiffs and Subclass Members for actual damages sustained by AT&T-Direct Plaintiffs and Subclass Members in consequence of AT&T's violations of Section 551, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher.

317. The AT&T-Direct Defendants are also liable for AT&T-Direct Plaintiffs' reasonable attorneys' fees and other litigation costs reasonably incurred pursuant to 47 U.S.C. § 551(f)(2)(C).

COUNT 4
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Classes against all Defendants)

318. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 278 above and incorporate the same as if set forth herein.

319. Plaintiffs bring this Count on behalf of the Nationwide Classes under the laws of the state of Texas, or in the alternative, under each state's respective common law.

320. Plaintiffs and Class Members entered into an implied contract with AT&T when they subscribed or purchased services from AT&T and provided their PII to AT&T.

321. By collecting PII from its customers, AT&T impliedly agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or compromised. Plaintiffs and Class Members believed that AT&T would use part of the monies paid to AT&T under the agreements or the monies obtained from AT&T's use of the PII to fund proper and reasonable data security practices. Plaintiffs and Class Members would have paid less for AT&T products or services in the absence of the implied contract or implied terms between them and AT&T. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

322. Specifically, AT&T impliedly agreed and expressly stated in all applicable Privacy Policies that, in exchange for Plaintiffs' and Class Members' provision of PII, AT&T would, among other obligations, maintain safeguards designed to protect the PII it collected, limit access to the PII to necessary personnel, and give timely and accurate notification if a breach occurs.

323. Plaintiffs and Class Members fully performed their obligations under the express and/or implied agreements with AT&T by providing their PII and making relevant payments.

324. AT&T materially breached its express and/or implied agreement with Plaintiffs and Class Members by failing to protect their PII and call, text, and location records. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) allowed Plaintiffs' and Class Members' PII to be disclosed to unauthorized third parties; (3) failed to timely notify Plaintiffs and Class Members of the Breach; and (4) failed to provide adequate information regarding the Breach in order for Plaintiffs and Class Members to undertake proper precautionary measures, in violation of the Agreements.

325. As a direct and proximate result of AT&T's breach of the express and/or implied agreements, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT 5
NEGLIGENCE
(On Behalf of the Nationwide Classes against all Defendants)

326. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 278 above and incorporate the same as if set forth herein.

327. Plaintiffs bring this Count on behalf of the Nationwide Classes under the laws of the state of Texas, or in the alternative, under each States' respective common law.

328. AT&T required Plaintiffs and Class Members to submit sensitive PII in order to obtain AT&T's products and services and also collected and stored sensitive personal information such as call, text, and location information about its customers and those of its MVNOs, on its own, either automatically as customers used AT&T's products and services, or through third-party data sources.

329. AT&T had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

330. AT&T owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing AT&T's security systems to ensure that Plaintiffs' and Class Members' PII in AT&T's possession was properly secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusion to its networks; (d) maintaining security measures consistent with industry standards discussed herein; and (e) failing to delete customer PII that AT&T no longer reasonably needed to keep, particularly as to former customers.

331. AT&T's duty to use reasonable care arose from several sources, including but not limited to the following:

a. AT&T holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiffs and Class Members. Because of its role as one of the largest telecommunications companies, AT&T was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the AT&T Data Breach. AT&T's own privacy policies set forth some of the duties it assumed when obtaining customers' PII;

b. AT&T's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable

measures to protect PII by companies such as AT&T. Various FTC publications and data security breach orders and Consent Decrees further form the basis of AT&T's duty. In addition, individual jurisdictions have enacted statutes either based upon the FTC Act that also created a duty or that incorporate similar duties, as alleged below. *See, e.g.*, Cal Civ. Code § 1798.100; Cal. Civ. Code § 1798.80; 815 Ill. Comp. Stat. § 530/10(a); Tex. Bus. & Com. Code § 521.052;

c. AT&T violated Section 5 of the FTC Act and similar state consumer protection statutes by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. AT&T's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Classes. Plaintiffs and Class Members were within the class of persons the FTC Act and similar state consumer protection statutes were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against. Thus, AT&T's violation of Section 5 of the FTC Act and similar statutes constitutes negligence;

d. As a cable operator providing cable services over a cable system through its U-Verse technology, AT&T's duties also arose under the Cable Communications Privacy Act ("Cable Act"), 47 U.S.C. §§ 521, *et seq.*, which required AT&T to "take such actions as are necessary to prevent unauthorized access to such [personally identifiable information concerning any subscriber] by a person other than the subscriber or cable operator," 47 U.S.C. § 551(c)(1), and to "destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected." 47 U.S.C. § 551(e). AT&T's conduct described herein violated these duties. Plaintiffs and Class Members are subscribers under the Cable Act and thus

are within the class of persons entitled to protection under the statute and the type of harm that resulted from the Data Breach was the type of harm that the statute was intended to guard against;

e. Furthermore, as a telecommunications carrier under the Communications Act of 1934 (“Communications Act”), 47 U.S.C. § 151, *et seq.*, AT&T “has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers[.]” 47 U.S.C. § 222(a). Specifically, AT&T “shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.” 47 U.S. Code §§ 222(c)(1), 201(B). AT&T’s conduct described herein violated this duty. Plaintiffs and Class Members are customers under the Communications Act and thus are within the class of persons entitled to protection under the statute and the type of harm that resulted from the Data Breach was the type of harm that the statute was intended to guard against;

f. AT&T also had a duty to safeguard the PII of Plaintiffs and Class Members and to promptly notify them of a breach pursuant to state statutes that require AT&T to reasonably safeguard sensitive PII. *See, e.g.*, C.G.S.A. § 42-110b; Kan. Stat. Ann. §§ 50-7a02(a); Ky. Rev. Stat. Ann. § 365.732; La. Rev. Stat. Ann. § 51:3074(A); Mich. Comp. Laws Ann. § 445.72; N.J. S.A. § 56:8-163; Tenn. Code Ann. § 47-18-2107; and Va. Code Ann. § 18.2-186.6;

g. AT&T had common law duties to prevent foreseeable harm to Plaintiffs and Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by AT&T’s failure to protect their PII because

hackers routinely attempt to steal such information and use it for nefarious purposes and had targeted AT&T's data systems prior to the Data Breaches; and

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

332. AT&T was required to provide timely, adequate, and appropriate notification of the Data Breaches to Plaintiffs and Class Members. As discussed above, Plaintiffs and Class Members needed timely and effective notice so they could take appropriate measures to prevent, mitigate, or ameliorate the damage caused by AT&T's misconduct. Had they known of the Data Breaches earlier and received more detailed information about it, Plaintiffs and Class Members could have taken such measures—including freezing or locking credit profiles, avoiding or reversing unauthorized charges to credit or debit card accounts, cancelling or changing usernames and passwords on compromised accounts, monitoring financial and other accounts and credit reports for fraudulent activity, contacting the banks or other financial institutions that issue their credit or debit cards, obtaining credit monitoring services, and other steps—earlier.

333. AT&T was subject to these “independent duties,” untethered to any contract between AT&T and Plaintiffs and Class Members.

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

misusing confidential PII in light of the history of breaches of AT&T's systems that AT&T has repeatedly allowed to occur.

335. AT&T breached the duties it owed to Plaintiffs and Class Members described above and thus was negligent. AT&T breached these duties by, among other things, failing to: (a) exercise reasonable care and implement proper security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the Data Breaches while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breaches; (d) comply with federal regulations protecting the PII at issue during the period of the Data Breaches; (e) disclose in a timely and adequate manner that Plaintiffs' and Class Members' PII in AT&T's possession had been, or was reasonably believed to have been, stolen or compromised; and (f) delete customer PII that AT&T no longer reasonably needed to keep, particularly as to its former customers.

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

337. Plaintiffs and Class Members had no ability to protect their PII that was in, and possibly remains in, AT&T's possession.

338. AT&T was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breaches.

339. Defendant's duty extended to protecting Plaintiffs and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place

to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts §302B (1965). Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

340. But for AT&T's wrongful and negligent breach of its duties, Plaintiffs' and Class Members' PII would not have been compromised and sold on the Dark Web.

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

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

COUNT 6
DECLARATORY AND INJUNCTIVE RELIEF
28 U.S.C. §§ 2201, *et seq.*
(On Behalf of the Nationwide Classes against All Defendants)

343. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 278 and incorporate the same as if set forth herein.

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

345. An actual controversy has arisen in the wake of the AT&T-Direct and AT&T-Snowflake Data Breaches regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and AT&T's failure to maintain data security measures that effectively protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future given the nature and quantity of the PII stored by AT&T and AT&T's repeated failure to maintain adequate data security measures resulting in numerous data breaches, as described in detail herein.

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

- a. AT&T continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act;
- b. AT&T continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. As a result of AT&T's ongoing breach of this legal duty, Plaintiffs and Class Members remain subject to continuing and imminent risk of harm.

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

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

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

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

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all Members of the proposed Nationwide Class and/or Subclass(es), respectfully request that the Court enter judgment in Plaintiffs' favor and against AT&T as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure;
- B. That the Court grant permanent injunctive relief to prohibit AT&T from continuing to engage in the unlawful acts, omissions, and practices described herein.
- C. That the Court determine that any alleged agreements to arbitrate or not to participate in a class action are deemed unenforceable;
- D. That the Court award Plaintiffs and Class Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;
- 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 the Court award statutory damages, treble, and punitive or exemplary damages, to the extent permitted by law;
- G. That Plaintiffs be granted the declaratory relief sought herein;
- H. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- I. That the Court award pre- and post-judgment interest at the maximum legal rate; and
- J. That the Court grant all such other relief as it deems just and proper.

JURY TRIAL DEMANDED

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs demand a jury trial as to all issues triable by a jury.

Dated: May 30, 2025

Respectfully submitted,

/s/ W. Mark Lanier

W. Mark Lanier

THE LANIER LAW FIRM, P.C.

10940 W. Sam Houston Pkwy N. Ste. 100

Houston, Texas 77064

Tel: (713) 659-5200

Email: mark.lanier@lanierlawfirm.com

Lead and Liaison Counsel for MDL 3114

Shauna Itri

SEEGER WEISS, LLP

55 Challenger Road

Ridgefield Park, New Jersey 07660

Tel: (973) 639-9100

Email: sitri@seegerweiss.com

James E. Cecchi

Jason H. Alperstein

Jordan M. Steele

CARELLA, BYRNE, CECCHI,

OLSTEIN, BRODY & AGNELLO, P.C.

5 Becker Farm Road

Roseland, New Jersey 07068

Tel: (973) 994-1700

Email: jcecchi@carellabyrne.com

Email: jalperstein@carellabyrne.com

Email: jsteele@carellabyrne.com

Jean Sutton Martin

MORGAN & MORGAN

COMPLEX LITIGATION GROUP

201 N Franklin Street 6th Floor

Tampa, Florida 33602

Tel: (813) 559-4908

Email: jeanmartin@forthepeople.com

Sean S. Modjarrad
Matthew P. Gigliotti
MODJARRAD ABUSAAD & SAID
212 W Spring Valley
Road Richardson, Texas 75081
Tel: (972) 789-1664
Email: smodjarrad@mas.law
Email: mgigliotti@mas.law

*Attorneys for Plaintiffs and Members of
Plaintiffs' Executive Committee*

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, Pennsylvania 19106
Tel: (215) 592-1500
Email: cschaffer@lfsblaw.com

Joseph P. Guglielmo
Erin Green Comite
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, New York 10169
Tel: (212) 776-8259
Email: jguglielmo@scott-scott.com
Email: ecomite@scott-scott.com

Larry A. Golston, Jr.
**BEASLEY, ALLEN, CROW, METHVIN,
PORTIS & MILES, P.C.**
272 Commerce Street
Montgomery, Alabama 36104
Tel: (334) 269-2343
Email: larry.golston@beasleyallen.com

Nicholas R. Lange
**FREED KANNER LONDON
& MILLEN LLC**
100 Tri-State International Drive, Suite 128
Lincolnshire, Illinois 60069
Tel: (224) 632-4510
Email: nlange@fkmlmlaw.com

Rebecca L. Solomon
TOUSLEY BRAIN STEPHENS PLLC
1200 5th Ave, Ste 1700
Seattle, Washington 98101
Tel: (206) 682-5600
Email: rsolomon@tousley.com

Thomas E. Loeser
COTCHETT PITRE & MCCARTHY LLP
999 N Northlake Way, Suite 215
Seattle, Washington 98103
Tel: (206) 970-8181
Email: tloeser@cpmlegal.com

*Attorneys for AT&T-Direct Plaintiffs, and
Members of Plaintiffs' Steering Committee*

/s/ Jason S. Rathod
Jason S. Rathod
MIGLIACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Tel: (202) 470-3520
Email: jrathod@classlawdc.com

/s/ John Heenan
John Heenan
HEENAN & COOK
1631 Zimmerman Trail
Billings, Montana 59102
Tel: (406) 839-9091
Email: john@lawmontana.com

/s/ Raphael Graybill
Raphael Graybill
GRAYBILL LAW FIRM, PC
300 4th Street North
Great Falls, Montana 59401
Tel: (406) 452-8566
Email: raph@graybilllawfirm.com

/s/ J. Devlan Geddes

J. Devlan Geddes

GOETZ, GEDDES & GARDNER P.C.

35 N. Grand Ave.

Bozeman, Montana 59715

Tel: (406) 587-0618

Email: devlan@goetzlawfirm.com

/s/ Jeff Ostrow

Jeff Ostrow

KOPELOWITZ OSTROW P.A.

One West Las Olas Blvd., Suite 500

Fort Lauderdale, Florida 33301

Tel: (954) 332-4200

Email: ostrow@kolawyers.com

Attorneys for AT&T-Snowflake Plaintiffs

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [\\$177 Million AT&T Settlement Resolves Data Breach Lawsuit Over Two 2024 Cyberattacks](#)
