UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Fulvia BANU, individually and on behalf of all those similarly situated, Plaintiff, v. AT&T Inc., Defendant.	)	Case No.:24cv61047 **CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

Plaintiff, Fulvia Banu ("Banu" or "Plaintiff") as an individual and on behalf of all others similarly situated ("Class"), brings this Class Action Complaint against the above-named AT&T Inc., a Texas Corporation, ("AT&T" or "Defendant"), and alleges, upon Personally knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this action against AT&T on behalf of all consumers nationwide against Defendant, for its failure to properly secure and safeguard her sensitive information.

2. Defendant is a major telecommunication corporation headquartered in Dallas, TX and Plaintiffs are AT&T customers who directly or indirectly entrusted their confidential personal information to AT&T.

3. In the course of providing its services, Defendant collected the personal information of its customers, including that of Plaintiff and the Class.

4. As a result of Defendant's failure to implement and maintain reasonable data security measures, an external actor was able to gain unauthorized access to Defendant's systems and access the data Defendant collected from Plaintiffs and the Class members. The unauthorized actor was able to access, exfiltrate, and steal the Personally Identifiable Information of Plaintiff and Class members (the "Data Breach")

5. At some time before March 17, 2024, Plaintiffs information was among the data accessed by the unauthorized third-party in the Data Breach.

6. The private information compromised in the Data Breach included Plaintiff's and Class Members' full names, mailing addresses, email addresses, phone numbers, dates of birth, and Social Security numbers ("Personally Identifiable Information" or "PII").

7. Personally Identifiable Information are representations of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

8. The Personally Identifiable Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves. In a dataset released on March 17, cyber-criminals sold such information on the dark web.

9. As a result of the Data Breach, Plaintiff and the Class Members, suffered concrete injuries in fact including, but not limited to: invasion of privacy; theft of their Personally Identifiable Information; lost or diminished value of Personally Identifiable Information; lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails, as well as financial fraud.

10. Plaintiff's Personally Identifiable Information remains unencrypted and available for unauthorized third parties to access and abuse; and remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personally Identifiable Information.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Class Member's Personally Identifiable Information from a foreseeable and preventable cyber-attack.

12. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to the fact that it collects and maintains highly valuable Private

Information on its systems. A 2023 report from cyber intelligence firm Cyble said that U.S. telecommunications companies are a lucrative target for hackers[1].

13. Defendant disregarded the rights of Plaintiff and Class Members by, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

14. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained has been accessed and acquired by data thieves.

15. By using the Personally Identifiable Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud by selling the data on the dark web. In the future criminals may, and probably will, commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

[1] https://cyble.com/blog/u-s-telecommunications-companies-targeted-consumers-hit-hardest/ (last visited June 15, 2024).

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members may also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

19. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

20. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

//

THE PARTIES

Plaintiff

21. Plaintiff, Fulvia Banu, is an individual residing in Broward County, Florida and is otherwise *sui juris.* Plaintiff received a Notice of Data Breach letter from AT&T, dated April 25, 2024, by U.S. Mail. Plaintiff provided her Personally Identifiable Information to AT&T prior to June 2019 and periodically updated such PII, when requested.

Defendant

22. Defendant, AT&T Inc., is incorporated in the State of Texas and its principal place of business is at Whitacre Tower (One AT&T Plaza), 208 S Akard St, Dallas, TX 75201, in Downtown Dallas, Texas. It is the world's fourth-largest telecommunications company by revenue and the largest wireless carrier in the United States.

JURSIDICTION AND VENUE

23. This Court has jurisdiction over the subject matter of this civil action pursuant to 28 U.S.C. § 1332(d). This is a putative class action whereby: (i) the proposed nationwide class consists of more than 100 members; (ii) at least one class member has a different citizenship from Defendant; and (iii) the claims of the proposed class exceed $5,000,000 in the aggregate.

24. The Court has personal jurisdiction over the Defendant due to its continuous and systemic contacts with the State of Florida.

25. Venue is proper in the Southern District of Florida, pursuant to 28 U.S.C. § 1391(b)(2). At all relevant times the Plaintiff resided in Davie, Florida, which is located in Broward County, within the Southern District of Florida. A substantial part of the events or omissions giving rise to the claim occurred in Broward County.

BACKGROUND FACTS

26. Defendant AT&T has millions of customers for its residential and business telecommunication services.

27. At some time before March 17, 2017, cyber criminals accessed data stored by AT&T, including names, dates of birth, physical ad email addresses, phone numbers, and Social Security numbers.

28. On March 26, 2024, Defendant determined that its customer information was included in a dataset released on the dark web on March 17, 2024.

29. Based on the Notice of Data Breach sent to Plaintiff, AT&T knows that the information illegally accessed includes: full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and AT&T passcode.

30. By obtaining, collecting, utilizing, and deriving a benefit from Plaintiff's and Class Members' Personally Identifiable Information, Defendant owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations to keep Plaintiff's and Class Members' Personally Identifiable Information

confidential, safe, secure, and protected from the unauthorized access, disclosure, and theft in foreseeable data breach incidents.

31. Defendant, however, disregarded its duties and obligations and the privacy rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable data security measures to protect and safeguard the Personally Identifiable Information of Plaintiff and Class Members, but rather allowed the Personally Identifiable Information to be stored and maintained in a vulnerable state.

32. But for Defendant's acts and omissions, the Data Breach would not have happened, and Plaintiff and Class Members would not have been injured as described herein.

AT&T Collects Personally Identifiable Information

33. Defendant collects the Personally Identifiable Information of its clients' customers as a condition of providing services. This Personally Identifiable Information is used by Defendant in the ordinary course of its business.

34. The types of Personally Identifiable Information collected and utilized by Defendant includes, at least, names, contact information, financial information, and Social Security numbers.

Defendant's Privacy Policy & Promises

35. On its customer-facing website, Defendant has a posted Privacy Policy available at: https://about.att.com/privacy.html

36. The Privacy Policy discusses the types of information AT&T collects and the reasons that it might use that information. Defendant lists a number of instances when it might share or disclose the Personally Identifiable Information entrusted to it without permission, none of which are applicable here.

The Data Breach

37. According to AT&T, on March 26, 2024, it became aware that it's consumer data was sold on the dark web as part of a "dataset".

38. AT&T claims that the Data Breach is impacting approximately 7.6 million current AT&T account holders and 65.4 million former account holders[2].

The Data Breach was Foreseeable and Preventable

39. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense" against data breaches and it is "critical to take precautions for [data] protection."[3]

40. Defendant has not publicly shared details of the Data Breach. However, based on Defendant's limited statements, it is clear Defendant did not take reasonable precautions that would have allowed it to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach. These failures allowed cybercriminals to

[2] https://www.att.com/support/article/my-account/000101995 (last visited June 16, 2024).

[3] *See* How to Protect Your Networks, available at https://www.fbi.gov/file-repository /ransomware-prevention-and-response-for-cisos.pdf/ view (last visited June 16, 2024).

access and steal the Personally Identifiable Information Defendant maintained on Plaintiff and Class Members.

41. Defendant could have prevented the Data Breach by encrypting the systems and files containing the Personally Identifiable Information of Plaintiff and Class Members and by destroying Personally Identifiable Information it no longer had a legitimate need for.

42. Additionally, to prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures known to be generally effective at mitigating the risk of a cyberattack:

a) Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b) Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c) Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

d) Configure firewalls to block access to known malicious IP addresses.

e) Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f) Set anti-virus and anti-malware programs to conduct regular scans automatically.

g) Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h) Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

i) Execute operating system environments or specific programs in a virtualized environment

j) Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

k) Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

l) Consider disabling Remote Desktop protocol (RDP) if it is not being

used.

m) Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

n) Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[4]

43. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

a) Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . .

b) Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses

[4] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 2, 2022).

(e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

c) Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d) Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

e) Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f) Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product

notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

g) Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[5]

44. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

a) Secure internet-facing assets: apply latest security updates; use threat and vulnerability management; perform regular audits; remove privileged credentials;

b) Thoroughly investigate and remediate alerts: prioritize and treat commodity malware infections as potential full compromise;

c) Include IT Pros in security discussions: ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

d) Build credential hygiene: use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local

[5] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2022).

admin passwords

e) Apply principle of least-privilege: monitor for adversarial activities; hunt for brute force attempts; monitor for cleanup of Event Logs; analyze logon events

f) Harden infrastructure: use Windows Defender Firewall and higher grade software; enable tamper protection; enable cloud-delivered protection; turn on attack surface reduction rules.[6]

45. Given that Defendant was storing the Personally Identifiable Information of Plaintiff and Class Members, Defendant could and should have implemented, at a minimum, all of the above measures to prevent and detect cyberattacks.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures and additional supplemental measures to prevent cyberattacks, resulting in the Data Breach and the unauthorized exposure and exfiltration of the Personally Identifiable Information of Plaintiff and Class Members.

47. Despite the prevalence of public announcements of data breach in the communication industry and data security compromises, Defendant failed to take

[6] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2022).

appropriate steps to protect the Personally Identifiable Information of Plaintiff and Class Members from being compromised.

Value of Personally Identifiable Information

48. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013). 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." *Id.*

49. The Personally Identifiable Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[7] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[8] Criminals can also purchase access

[7] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited June 16, 2024).

[8] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 16, 2024).

to entire company data breaches from $900 to $4,500.[9]

50. AT&T does not say in this letter what was the price paid on the dark web for the dataset including the personal information of the Plaintiff and Class Members.

51. Social Security numbers are among the worst kind of Personally information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[10]

52. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted;

---

[9] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 16, 2024).

[10] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 16, 2024).

an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

53. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[11]

54. Based on the foregoing, the Personally Identifiable Information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The Information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change: Social Security number and name.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

---

[11] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 16, 2024).

[12] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 16, 2024).

56. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

57. The fraudulent activity resulting from the Data Breach may not come to light for years.

58. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Personally Identifiable Information of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. The ramifications of Defendant's failure to keep secure the Personally Identifiable Information of Plaintiff and Class Members are long lasting and severe.

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited June 16, 2024).

Once Personally Identifiable Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages, in addition to any fraudulent use of their Personally Identifiable Information.

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. To date, Defendant has offered Plaintiff and Class Members only 12 months of credit monitoring, identity restauration and few ancillary services through Experian's IdentityWorks[SM]. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Personally Identifiable Information at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services that it offered.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personally Identifiable Information of Plaintiff and Class Members.

64. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Personally Identifiable Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Personally Identifiable Information from unauthorized disclosure.

65. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Personally Identifiable Information.

66. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Personally Identifiable Information confidential and securely maintained, to use such Personally Identifiable Information solely for business and purposes, and to prevent the unauthorized disclosures of the Personally Identifiable Information.

Defendant Failed to Comply with FTC Guidelines

67. Defendant was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff' and Class Members' Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information stored within its systems because of its position as a leading business affiliate to a variety of companies. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff Banu's Experience

71. Prior to the Data Breach, Defendant retained Plaintiff Banu's name, contact information, financial information, and Social Security number.

72. Plaintiff Banu provided her Personally Identifiable Information to Defendant with the expectation that her Personally Identifiable Information would remain confidential.

73. Plaintiff Banu trusted that her Personally Identifiable Information would be safeguarded according to internal policies and state and federal law.

74. Upon information and belief, Plaintiff Banu's Personally Identifiable Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

75. On approximately April 25, 2024, Defendant notified Plaintiff that AT&T Customer information was included in a dataset released on the dark web o March 17, 2024.

76. Shortly after receiving the notice, Plaintiff Banu realized that someone else opened a Chase bank account on her name. Plaintiff spent time to investigate and ultimately try to close the ghost account. While Plaintiff is not aware of other new accounts opened in her name by unknown individuals, it is obvious that criminals have the ability to open accounts on her name.

77. Plaintiff Banu is very careful about sharing her sensitive Personally Identifiable Information. Plaintiff Banu has never knowingly transmitted unencrypted sensitive Personally Identifiable Information over the internet or any other unsecured source. Plaintiff Banu stores any documents containing her Personally Identifiable Information in a safe and secure location or destroys the documents.

CLASS ALLEGATIONS

78. Plaintiffs bring this action as a class pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of the following class:

> National Class: All individuals residing in the United States whose Personally Identifiable Information was accessed and/or acquired by an

unauthorized party as a result of the data breach reported by Defendant in April 2024 (the "Class").

79. The class excludes counsel representing the class, governmental entities, Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns, any judicial officer presiding over this matter, the members of their immediate families and judicial staff, and any individual whose interests are antagonistic to other putative class members.

80. Plaintiffs reserve the right to amend or modify the class descriptions with greater particularity or further division into subclasses or limitation to particular issues.

81. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23 because it is a well-defined community of interest in the litigation and the class is readily and easily ascertainable.

Numerosity

82. The potential members of the class are so numerous that joinder of all members of the class is impractical. Although the precise number of putative class members has not been determined at this time, Plaintiff is informed and believes that that the proposed class includes thousands of members.

Predominance

83. There are common questions of law and fact that predominate over any questions affecting only individual putative class members.

Typicality

84. Plaintiffs' claims are typical of the claims of the members of the putative class because every Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

Superiority of Class Action

85. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of putative class members is not practicable and questions of law and fact common to the class members predominate over any questions affecting only individual putative class members.

86. Each member of the putative class has been damaged and is entitled to recovery by reason of Defendant's illegal acts.

87. Class action treatment will allow those similarly situated to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system.

88. Plaintiffs are unaware of any difficulties that are likely to be construed in the management of this action that would preclude its maintenance as a class action.

89. The disposition of all claims of the members of the class in a class action, rather than individual actions, benefits the parties and the Court. The interests of the class members in controlling prosecution of separate claims against the Defendant is small when compared to the efficiency of a class action.

Adequacy of Representation

90. Plaintiff Banu will fairly and adequately represent and protect the interests of the class. Counsel for Plaintiff and for the putative class members are experienced litigators, competent in litigating class actions, and able to litigate this action on behalf of the class.

CLAIMS FOR RELIEF

COUNT I – BREACH OF FIDUCIARY DUTY

91. The allegations contained in Paragraphs 1 – 90 of the Complaint are incorporated by reference as if fully set out herein.

92. Plaintiffs assert this count on their own behalf and on behalf of all other similarly situated persons members of the National Class.

93. Because of the special relationship between Defendant and Plaintiff and Class, Defendant became a fiduciary by its undertaking and guardianship of the Personally Identifiable Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Personally Identifiable Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

94. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with Medicare beneficiaries, in particular, to keep secure their Personally Identifiable Information.

95. Defendant breached its fiduciary duties to Plaintiff and Class Members

by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

96. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Personally Identifiable Information.

COUNT II – NEGLIGENCE

97. The allegations contained in Paragraphs 1 through 90 of the Complaint are incorporated by reference as if fully set out herein.

98. Plaintiff Banu asserts this count on her own behalf and on behalf of all other similarly situated persons members of the National Class.

99. Plaintiff and the Class members entrusted their Personally Identifiable Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Personally Identifiable Information for business purposes only, and/or not disclose their Personally Identifiable Information to unauthorized third parties.

100. Defendant had full knowledge of the sensitivity of the Personally Identifiable Information and the types of harm that Plaintiff and the Class could and would suffer if the Personally Identifiable Information were wrongfully disclosed.

101. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personally Identifiable Information of Plaintiff and the Class involved an unreasonable risk of harm to

Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

102. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

103. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Personally Identifiable Information of Plaintiff and the Class.

104. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Personally Identifiable Information, a necessary part of obtaining services from Defendant. That duty further arose because Defendant chose to collect and maintain the Personally Identifiable Information for its own pecuniary benefit.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class members.

106. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and other security breach incidents at other similar providers of telecommunication services.

107. Plaintiff and the Class's injuries were the foreseeable and probable result of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personally Identifiable Information of Plaintiff and the Class, the critical importance of providing adequate security of that Personally Identifiable Information, and the necessity for encrypting Personally Identifiable Information stored on Defendant's systems.

108. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class.

109. Plaintiff and the Class had no ability to protect their Personally Identifiable Information that was within, and on information and belief remains within, Defendant's possession.

110. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class members as a result of the Data Breach.

111. Defendant had (and continues to have) a duty to timely and adequately disclose that the Personally Identifiable Information of Plaintiff and the Class members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personally Identifiable Information by third parties.

112. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Personally Identifiable Information of Plaintiff and the Class members.

113. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personally Identifiable Information of Plaintiff and the Class during the time the Personally Identifiable Information was within Defendant's possession or control.

114. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personally Identifiable Information of Plaintiff and the Class in the face of increased risk of theft.

115. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Personally Identifiable Information.

116. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Personally Identifiable Information of Plaintiff and the Class members would not have been compromised.

117. There is a close causal connection between Defendant's failure to implement adequate data security measures to protect the Personally Identifiable Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Personally Identifiable Information of

Plaintiff and the Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personally Identifiable Information by adopting, implementing, and maintaining appropriate security measures.

118. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personally Identifiable Information and by not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personally Identifiable Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

119. Defendant's violation of Section 5 of the FTC Act is, in and of itself, evidence of Defendant's negligent data security practices.

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

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

122. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: actual

identity theft; the loss of the opportunity to decide how their Personally Identifiable Information is used; the compromise, publication, and/or theft of their Personally Identifiable Information; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personally Identifiable Information; lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; costs associated with placing freezes on credit reports; the continued risk to their Personally Identifiable Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personally Identifiable Information of Plaintiff and the Class; and present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Personally Identifiable Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

123. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

124. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class members have suffered and will suffer the continued risks of exposure of their Personally Identifiable Information, which remains in Defendant's possession and is subject to further unauthorized disclosures on the dark web, so long as Defendant continues to fail to undertake appropriate and adequate data security measures to protect the Personally Identifiable Information.

125. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III – BREACH OF IMPLIED CONTRACT

126. The allegations contained in paragraphs 1 through 90 of the Complaint are incorporated by reference as if fully set out herein.

127. The named Plaintiff asserts this count on her own behalf and on behalf of the National class, as defined above.

128. Defendant required Plaintiff and the Class to provide and entrust their Personally Identifiable Information, including, without limitation, first and last name, contact information, financial account numbers, and Social Security numbers.

129. Defendant solicited and invited Plaintiff and the Class to provide their Personally Identifiable Information to Defendant, as part of Defendant's regular business practices. Plaintiff and the Class accepted Defendant's offers and provided their Personally Identifiable Information to Defendant.

130. As a condition of obtaining care and/or services from Defendant's clients, Plaintiff and the Class provided and entrusted Defendant with their Personally Identifiable Information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

131. A meeting of the minds occurred when Plaintiff and the Class agreed to, and did, provide their Personally Identifiable Information to Defendant with the reasonable understanding that their Personally Identifiable Information would be adequately protected from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive Personallyly Identifiable Information exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiff and Class Members would not have provided their Personally Identifiable Information.

132. Defendant separately has contractual obligations arising from and/or supported by the consumer facing statements in its Privacy Policies.

133. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

134. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their Personally Identifiable Information and

by failing to provide timely and accurate notice that Personally Identifiable Information was compromised as a result of the Data Breach. The notice provided merely stated that Plaintiff's Personally Identifiable Information os available for sale on the dark web.

135. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

136. As a result of Defendant's breach of implied contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV – UNJUST ENRICHMENT/RESTITUTION

137. The allegations contained in paragraphs 1 through 90 of the Complaint are incorporated by reference as if fully set out herein.

138. The named Plaintiff asserts this count on her own behalf and on behalf of the National class, as defined above.

139. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant, directly or indirectly, with their valuable Personally Identifiable Information.

140. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' Personally Identifiable Information.

141. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

142. Under the principles of equity, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

143. Defendant acquired the monetary benefit and Personally Identifiable Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

144. If Plaintiff and Class Members knew that Defendant had not secured their Personally Identifiable Information, they would not have agreed to provide their Personally Identifiable Information to Defendant.

145. Plaintiff and Class Members have no adequate remedy at law.

146. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: actual identity theft; the loss of the opportunity how their Personally Identifiable Information is used; the compromise, publication, and/or theft of their Personally Identifiable Information; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personally Identifiable Information; lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; time and effort spent to close ghost accounts, the continued risk to their Personally Identifiable Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Personally Identifiable Information in their continued possession and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personally Identifiable Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

147. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

148. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them

RELIEF REQUESTED

WHEREFORE, Plaintiff, Fulvia Banu, respectfully requests that this Court enter judgment in her favor and in favor of those similarly situated, as follows:

1. Certifying and maintaining this action as a class action, with the named Plaintiffs as designated class representative and with her counsel appointed as class counsel;

2. A declaration that Defendant is in violation of each of the Counts set forth above;

3. Award Plaintiffs and those similarly situated statutory, compensatory, and treble damages;

4. Award Plaintiffs and those similarly situated liquidated damages;

5. Order the disgorgement of illegally obtained monies;

6. Award the named Plaintiffs a service award;

7. Award attorneys' fees and costs; and

8. Grant such further relief as the Court deems just and proper.

Dated: June 18, 2024

Respectfully submitted,

s/Bogdan Enica
Bogdan, Enica
FL Bar No.: 101934
1200 N Federal Hwy. Ste.375
Boca Raton, FL 33432
Telephone: (305) 306-4989
Email: bogdan@keithgibsonlaw.com

Keith L. Gibson (*Pro Hac Vice* forthcoming)
IL Bar No.: 6237159
490 Pennsylvania Avenue Suite 1
Glen Ellyn, IL 60137
Telephone: (630) 677-6745
Email: keith@keithgibsonlaw.com

Counsel for Plaintiff and the Putative Class