AlaFile E-Notice

11-CV-2025-900178.00

To: HIRSCH JONATHAN RAYMOND
jhirsch@shb.com

NOTICE OF ELECTRONIC FILING

IN THE CIRCUIT COURT OF CALHOUN COUNTY, ALABAMA

GENIE PEMBROOK V. AOD FEDERAL CREDIT UNION
11-CV-2025-900178.00

The following complaint was FILED on 8/14/2025 4:22:40 PM

Notice Date: 8/14/2025 4:22:40 PM

KIM MCCARSON
CIRCUIT COURT CLERK
CALHOUN COUNTY, ALABAMA
25 WEST 11TH STREET
ANNISTON, AL, 36201

256-231-1750

ELECTRONICALLY FILED
8/14/2025 4:22 PM
11-CV-2025-900178.00
CIRCUIT COURT OF
CALHOUN COUNTY, ALABAMA
KIM MCCARSON, CLERK

IN THE CIRCUIT COURT FOR CALHOUN COUNTY, ALABAMA

IN RE AOD FEDERAL CREDIT UNION DATA BREACH LITIGATION	
	Case No. 11-CV-2025-900178
This Document Relates To: ALL ACTIONS	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Genie Pembrook, Judy Young, Nadja Britt, Julia Bullock, Diane Hollingsworth, and Gary Hollingsworth ("Plaintiffs") bring this Consolidated Class Action Complaint against AOD Federal Credit Union ("Defendant" or "AODFCU"), individually, and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This putative class action arises out of Defendant's failures to properly secure and safeguard the Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI")[2] (hereinafter, "Private Information") of Plaintiffs and other similarly situated customers of AODFCU, resulting in the unauthorized disclosure of that Private Information during a

[1] The Federal Trade Commission defines "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." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. U.S. Dep't of Health & Hum. Servs., *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws- regulations/index.html.

cyberattack in August 2024 (the "Data Breach").[3,4]

2. On information and belief, the Private Information unauthorizedly disclosed in the Data Breach includes Plaintiffs' and the Class Members' first and last names, Social Security Numbers, dates of birth, bank/financial account numbers, routing numbers, credit and/or debit card numbers, driver's license/government ID numbers, clinical or treatment information, health insurance member IDs and/or group numbers, and Taxpayer Identification Numbers.[5]

3. Headquartered in Bynum, Alabama, Defendant is a federal credit union that provides financial services to its members, including checking, savings, credit card, and lending services.[6]

4. As a condition of providing these services, Defendant requires that its customers provide AODFCU with their Private Information, which it promises to safeguard.

5. Defendant failed to undertake adequate measures to safeguard the Private Information of Plaintiffs and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

6. According to Defendant, it "detected unauthorized access to its network" on or about August 9, 2024, and astoundingly, its investigation lasted until March 4, 2025.[7] On information and belief, it was not until on or about March 27, 2025 that AODFCU began to send written notification to affected customers, but said notices failed to include key information,

[3] *See AOD Federal Credit Union ("AODFCU") Notice of Data Security Incident* (Mar. 2025), https://www.aodfcu.com/wp-content/uploads/2025/03/ADFCU-Website-Notice35665417.1.pdf.
[4] *See 2025-3-27 AOD Federal Credit Union Data Breach Notice to Consumers* (Mar. 27, 2025), https://ago.vermont.gov/sites/ago/files/documents/2025-03-27%20AOD%20Federal%20Credit%20Union%20Data%20Breach%20Notice%20to%20Consumers.pdf.
[5] *AOD Federal Credit Union Notice of Data Security Incident*, *supra* note 3.
[6] AOD Federal Credit Union, https://www.aodfcu.com (last visited Aug. 4, 2025).
[7] *AOD Federal Credit Union Notice of Data Security Incident*, *supra* note 3.

including the identity of the cybercriminals, or how the Data Breach occurred.

7. Indeed, Defendant has not disclosed what type of attack occurred or what vulnerability was exploited. This is typical of a breached company that simply failed to have sufficient cybersecurity measures—such as monitoring and alerting tools—in place such that it would be able to determine the answer to these questions.

8. Notably, forensics investigators cannot divine the root cause of breach or otherwise determine the full scope of what information was stolen or accessed if the company did have appropriate logging and monitoring systems in place *before* the incident began.

9. Moreover, Defendant waited about seven months to begin notifications, notwithstanding that it was required notify affected individuals within forty-five (45) days. Ala. Code § 8-38-5(b).

10. Defendant's failure to timely notify strongly suggests that it lacks a sufficient cybersecurity incident response plan, which is an elementary component of any reasonable cybersecurity program and is designed to ensure that companies can timely respond to breaches in compliance with the various data breach notification statutes that now exist in every state in the country.

11. Because of Defendant's failures, Plaintiffs and the proposed Class Members have suffered injuries and damages, including but not limited to severe invasions of privacy, and they must now face a substantially increased risk of identity theft and fraud for years to come, necessitating Plaintiffs to seek relief on a class wide basis.

PARTIES

12. Plaintiff Genie Pembrook is a resident and citizen of the State of Alabama, where she intends to remain, with a primary residence in Eastaboga, Alabama in Calhoun County.

13. Plaintiff Judy Young is a resident and citizen of the State of Alabama, where she intends to remain, with a primary residence in Anniston, Alabama in Calhoun County.

14. Plaintiff Nadja Britt is a resident and citizen of the State of Alabama, where she intends to remain, with a primary residence in Oxford, Alabama in Calhoun County.

15. Plaintiff Julia Bullock is a resident and citizen of the State of Alabama, where she intends to remain, with a primary residence in Eastaboga, Alabama in Calhoun County.

16. Plaintiff Diane Hollingsworth is a resident and citizen of the State of Alabama, where she intends to remain, with a primary residence in Anniston, Alabama in Calhoun County.

17. Plaintiff Gary Hollingsworth is a resident and citizen of the State of Alabama, where he intends to remain, with a primary residence in Anniston, Alabama in Calhoun County.

18. Defendant, AOD Federal Credit Union ("Defendant" or "AODFCU"), is a federal credit union with a principal place of business at 334 Victory Drive, Bynum, Alabama 36253 in Calhoun County.

19. On information and belief, Defendant's Registered Agent for Service of Process is David Mooney, 334 Victory Drive, Bynum, Alabama 36253.

JURISDICTION AND VENUE

20. Jurisdiction is proper in Alabama because, at all relevant times, AOD conducted (and continues to conduct) business in Alabama, Plaintiffs provided their Private Information to AOD in Alabama, Plaintiffs' Private Information was stored on AOD's computer networks, systems and/or servers in Alabama, many of AOD's wrongful acts and omissions took place in Alabama, and Defendant principal places of business are in Alabama.

21. Venue is proper in Calhoun County, Alabama pursuant to Ala. Code §§ 6-3-7(a) and (b) because, at all relevant times, Plaintiffs resided and continue to reside in Calhoun County,

because a substantial part of the events or omissions giving rise to this action occurred in Calhoun County, Defendant's principal place of business is in Calhoun County, and Defendant routinely conducts business throughout Calhoun County.

COMMON FACTUAL ALLEGATIONS

A. Defendant and the Data Breach

22. Defendant is a federal credit union with roots going back to 1950, which holds itself out as "a cooperative organized for members to pool their savings, lend them to one another, and own the organization where they save, borrow, and obtain related financial services."[8]

23. AODFCU provides myriad financial services to its members, including checking and savings accounts, credit cards, insurance, as well as lending for student loans, automobile loans, construction loans, mortgage loans, business loans, and more.[9]

24. Defendant provides services throughout Alabama at six (6) different locations, including in Bynum, Greenbrier, Jacksonville, Lenlock, Oxford, and in Pell City, Alabama.[10]

25. As a material condition of providing credit union financial services to its members, Defendant required that its customers—Plaintiffs and the Class Members—provide their Private Information, including their names, Social Security Numbers, dates of birth, bank/financial account numbers, routing numbers, credit and/or debit card numbers, driver's license/government ID numbers, clinical or treatment information, health insurance member IDs and/or group numbers, and Taxpayer Identification Numbers.

26. Defendant promises to protect the Private Information it required from its members, maintaining a Privacy Notice in which it states that:

The types of personal information we collect and share depend on the product or

[8] *History of AOD Federal Credit Union*, https://www.aodfcu.com/history.
[9] AOD Federal Credit Union, https://www.aodfcu.com.
[10] AOD Federal Credit Union, https://www.aodfcu.com/locations (last visited Aug. 4, 2025).

service you have with us. This information can include:

- Social Security number and account balances
- account transactions and checking account information
- payment history and transaction history[11]

27. Therein, Defendant further promises that it collects personal information when members open an account of use their credit or debit cards, show their government-issued ID or apply for financing or when member give Defendant their contact information. AODFCU further states that it collects personal information from others, such as credit bureaus, affiliates, or other companies.[12]

28. In its privacy practices, AODFCU affirmatively states that:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
>
> We maintain physical, electronic, and procedural safeguards that comply with federal regulations and leading industry practices to safeguard your nonpublic personal information.[13]

29. Accordingly, Defendant made representations to Plaintiffs and Class Members that their PHI would be kept safe and confidential, and that the privacy of that information would be maintained.

30. Defendant stored the Private Information of Plaintiffs and the Class in its computer systems. The Private Information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

31. Plaintiffs' and Class Members' Private Information was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

---

[11] *Privacy Policy of AOD Federal Credit Union*, https://www.aodfcu.com/privacy.
[12] *Id*.
[13] *Id*.

32. Defendant has admitted that it suffered a Data Breach from August 8, 2024 to August 9, 2024 in which its customers' Private Information was compromised, including their first and last names, Social Security Numbers, dates of birth, bank/financial account numbers, routing numbers, credit and/or debit card numbers, driver's license/government ID numbers, clinical or treatment information, health insurance member IDs and/or group numbers, and Taxpayer Identification Numbers.[14]

33. Indeed, Defendant states that "[o]n or about August 9, 2024, AODFCU detected unauthorized access to its network[;]" and that, thereafter Defendant purportedly "immediately secured the environment and commenced a prompt and thorough investigation […and…] also reported the incident to the Federal Bureau of Investigation […and…] has worked very closely with external cybersecurity professionals experienced in handling these types of incidents."[15]

34. On information and belief, it was not until on or about March 27, 2025, that AODFCU began to send written notification to affected customers, but said notices fail to include key information, including the identity of the cybercriminals, or how the Data Breach occurred.

35. Plaintiffs' Private Information was compromised in the Data Breach, including her name, Social Security Number, bank/financial account information, routing number, credit and/or debit card number was compromised in the Data Breach.

36. On information and belief, the Private Information unauthorizedly disclosed in the Data Breach includes Plaintiffs' and the Class Members' first and last names, Social Security Numbers, dates of birth, bank/financial account numbers, routing numbers, credit and/or debit card numbers, driver's license/government ID numbers, clinical or treatment information, health

[14] *AOD Federal Credit Union Notice of Data Security Incident*, *supra* note 3**.**
[15] *Id.*

insurance member IDs and/or group numbers, and Taxpayer Identification Numbers.[16]

37. Given its collection and storage of Private Information and because of the highly foreseeable risk of experiencing to Plaintiffs of a data breach if systems were vulnerable, Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumers' Private Information safe and confidential.

38. Moreover, the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA" or "FTC Act"), HIPAA, and industry standards further establish the standard of care required to keep Plaintiffs Private Information confidential and to protect it from unauthorized access and disclosure.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

B. Defendant's Data Breach Was Imminently Foreseeable

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

41. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

[16] *Id.*

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[17]

43. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members because of a breach.

44. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

45. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially hundreds of thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

46. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

47. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

C. Value of Personally Identifiable Information

48. Identity theft is "a fraud committed or attempted using the identifying information

[17] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s.

of another person without authority."[18] And "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."[19]

49. The PII 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.[20]

50. The information compromised in the Data Breach is even more significant because it includes health and medical information, which extraordinarily sensitive and private and is commonly used to perpetrate medical and insurance fraud.

51. 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 . . . [is] worth more than 10x on the black market."[21]

52. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII 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

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id.*
[20] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.
[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

> 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.[22]

D. Defendant Failed to Comply with FTC Guidelines

53. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the 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 Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

54. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any 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 someone is attempting to hack into 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.

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

security measures.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by 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 the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

58. Defendant was at all times fully aware of its obligation to protect the PII of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant'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 Class.

59. Moreover, the FTC has created a clearly defined standard of care that it expects all companies to follow to reasonably secure PII through the publication of guideline documents and through its many consent orders with companies through data breach enforcement actions. These consent orders are remarkably consistent and show the Commission's expectations for companies that collect and maintain sensitive PII.

E. Defendant Failed to Comply with Industry Standards.

60. Experts studying cybersecurity routinely identify institutions that store Private Information like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

61. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all these industry best practices.

62. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

63. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. Defendant failed to comply with these accepted standards, thereby permitting the

Data Breach to occur.

F. Common Injuries & Damages

65. Because of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

G. The Data Breach Increases Victims' Risk of Identity Theft and Fraud

66. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiffs' and Class Members' Private Information falling into the hands of identity thieves.

67. The unencrypted Private Information of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the Private Information for the express purpose of conducting financial fraud and identity theft operations.

68. Further, the standard operating procedure for cybercriminals is to use some data, like the PHI here, to access "fullz packages" of that person to gain access to the full suite of

additional PHI that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[23]

69. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

70. The development of "Fullz" packages means here that the stolen Private Information 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. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still 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.

H. Loss of Time to Mitigate Risk of Identity Theft and Fraud

71. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this

[23] "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 you have on a victim, the more money that 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 Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

72. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiffs' and Class Members' Private Information is affected because such information is commonly used to commit medical and insurance fraud.

73. By spending this time, data breach Plaintiffs are not manufacturing their own harm but are taking necessary steps at Defendant's direction and because the Data Breach included their Private Information.

74. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

75. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

[24] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

76. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

I. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

77. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims. Regardless, the data is already in the hands of unauthorized actors because of the Data Breach. Any further transfer of the Private Information represents an additional harm to Plaintiffs' privacy and even further increases the risk of future identity theft and financial fraud.

78. Such fraud may go undetected for years; consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

79. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiffs and Class Members would not need to bear but for

[25] *See* Fed. Trade Comm'n, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

Defendant's failure to safeguard their Private Information.

PLAINTIFFS' EXPERIENCES

Plaintiff Genie Pembrook

80. Plaintiff Pembrook provided her information to Defendant as a condition of becoming a customer of Defendant, including her Social Security number and financial account information, which upon information and belief, was then exposed to cybercriminals in the Data Breach.

81. Plaintiff Pembrook is very careful about sharing her sensitive Private Information. Plaintiff Pembrook has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

82. As a result of the Data Breach, Plaintiff Pembrook made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

83. Plaintiff Pembrook has spent significant time and will continue to spend valuable hours for the remainder of his life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

84. Moreover, Plaintiff Pembrook has experienced a significant increase in spam and scam messages since the Data Breach.

85. Plaintiff Pembrook suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Pembrook; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending

injury arising from the increased risk of identity theft and fraud.

86. As a result of the Data Breach, Plaintiff Pembrook has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Pembrook is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

87. As a result of the Data Breach, Plaintiff Pembrook anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

Plaintiff Judy Young

88. Plaintiff Young provided her information to Defendant as a condition of becoming a customer of Defendant, including her Social Security number and financial account information, which upon information and belief, was then exposed to cybercriminals in the Data Breach.

89. Plaintiff Young is very careful about sharing her sensitive Private Information. Plaintiff Young has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

90. As a result of the Data Breach, Plaintiff Young made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

91. Plaintiff Young has spent significant time and will continue to spend valuable hours

for the remainder of his life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

92. Moreover, Plaintiff Young has experienced a significant increase in spam and scam messages since the Data Breach.

93. Plaintiff Young suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Young; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

94. Indeed, the substantial risk of identity theft and fraud has already begun to occur for Plaintiff Young, who experienced two credit cards fraudulently opened in her name, which required her time and effort to resolve.

95. Moreover, Plaintiff Young had a fraudulent tax filing made in her name.

96. As a result of the Data Breach, Plaintiff Young has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Young is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

97. As a result of the Data Breach, Plaintiff Young anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

Plaintiff Diane Hollingsworth

98. Plaintiff D. Hollingsworth provided her information to Defendant as a condition of becoming a customer of Defendant.

99. Plaintiff D. Hollingsworth is very careful about sharing her sensitive Private Information. Plaintiff D. Hollingsworth has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

100. Plaintiff D. Hollingsworth first learned of the Data Breach after receiving a Notice of Data Breach letter from Defendant dated March 27, 2025.

101. The notification letter confirmed that her name, Social Security number, bank/financial account number, and credit/debit card numbers were included in the Data Breach.

102. As a result of the Data Breach, Plaintiff D. Hollingsworth made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

103. Plaintiff D. Hollingsworth has spent significant time and will continue to spend valuable hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

104. Indeed, the substantially increased risk of identity theft and fraud Plaintiff Hollingsworth has already started to come to fruition. Bad actors have already attempted to take money out of her bank account.

105. Moreover, Plaintiff D. Hollingsworth has experienced a significant increase in spam and scam messages since the Data Breach.

106. Plaintiff D. Hollingsworth suffered actual injury from having her PII compromised

as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff D. Hollingsworth; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

107. As a result of the Data Breach, Plaintiff D. Hollingsworth has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff D. Hollingsworth is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

108. As a result of the Data Breach, Plaintiff D. Hollingsworth anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff D. Hollingsworth will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

Plaintiff Gary Hollingsworth

109. Plaintiff G. Hollingsworth provided his information to Defendant as a condition of becoming a customer of Defendant.

110. Plaintiff G. Hollingsworth is very careful about sharing his sensitive Private Information. Plaintiff Hollingsworth has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

111. Plaintiff G. Hollingsworth first learned of the Data Breach after receiving a Notice of Data Breach letter from Defendant dated March 27, 2025.

112. The notification letter confirmed that her name, Social Security number,

bank/financial account number, and credit/debit card numbers were included in the Data Breach.

113. As a result of the Data Breach, Plaintiff G. Hollingsworth made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

114. Plaintiff G. Hollingsworth has spent significant time and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

115. Indeed, the substantially increased risk of identity theft and fraud Plaintiff G. Hollingsworth has already started to come to fruition. Bad actors have already attempted to take money out of his bank account, which required that he spend his valuable time to communicate with his bank and get a new payment card.

116. Moreover, Plaintiff G. Hollingsworth has experienced a significant increase in spam and scam messages since the Data Breach.

117. Plaintiff G. Hollingsworth suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff G. Hollingsworth; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

118. As a result of the Data Breach, Plaintiff G. Hollingsworth has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Hollingsworth is very

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

119. As a result of the Data Breach, Plaintiff G. Hollingsworth anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff G. Hollingsworth will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

Plaintiff Nadja Britt

120. Plaintiff Britt provided her information to Defendant as a condition of becoming an employee of Defendant in 2023, including her Social Security number and financial account information, which upon information and belief, was then exposed to cybercriminals in the Data Breach.

121. Plaintiff Britt is very careful about sharing her sensitive Private Information. Plaintiff Britt has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

122. As a result of the Data Breach, Plaintiff Britt made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

123. Plaintiff Britt has spent significant time and will continue to spend valuable hours for the remainder of his life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation. She has been forced to go through her personal accounts and change her passwords and continuously monitor her accounts and credit for fraudulent transactions.

124. Moreover, Plaintiff Britt has experienced a significant increase in spam and scam messages since the Data Breach. It is particularly concerning that her scam messages are focused on financial accounts, as that is the data she was informed was compromised in the breach.

125. Plaintiff Britt suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Britt; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

126. As a result of the Data Breach, Plaintiff Britt has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Britt is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

127. As a result of the Data Breach, Plaintiff Britt anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

Plaintiff Julia Bullock

128. Plaintiff Bullock provided her information to Defendant as a condition of becoming a customer of Defendant, including her Social Security number and financial account information, which upon information and belief, was then exposed to cybercriminals in the Data Breach.

129. Plaintiff Bullock is very careful about sharing her sensitive Private Information.

Plaintiff Bullock has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

130. As a result of the Data Breach, Plaintiff Bullock made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or other accounts for any indications of actual or attempted identity theft or fraud.

131. Plaintiff Bullock has spent significant time and will continue to spend valuable hours for the remainder of his life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

132. Moreover, Plaintiff Bullock has experienced a significant increase in spam and scam messages since the Data Breach. The increased messages are related to financial transactions, loans and/or opening credit accounts, which indicates to Plaintiff her financial information has been disseminated and unauthorized persons are attempting to utilize her data to open fraudulent accounts.

133. Plaintiff Bullock suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Bullock; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

134. As a result of the Data Breach, Plaintiff Bullock has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Bullock is very concerned about identity

theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

135. As a result of the Data Breach, Plaintiff Bullock anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

CLASS ALLEGATIONS

136. Plaintiffs bring this action on behalf of themselves and on behalf of all members of the proposed class defined as:

> **All resident citizens of the State of Alabama whose Private Information was compromised in the Data Breach ("Class").**

137. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

138. Plaintiffs reserve the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

139. The proposed Class meets the criteria certification under Alabama Rule of Civil Procedure 23.

140. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believe the proposed Class includes at least 70,000 individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's

records.

141. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- Whether Defendant engaged in the conduct alleged herein;
- Whether Defendant's conduct violated the FTC Act and HIPAA;
- When Defendant learned of the Data Breach;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;
- Whether Defendant owed duties to Class Members to safeguard their Private Information;
- Whether Defendant breached her duties to Class Members to safeguard her Private Information;
- Whether hackers obtained Class Members' Private Information via the Data Breach;
- Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- Whether Defendant breached its duty to provide timely and accurate notice of

the Data Breach to Plaintiffs and Class Members;

- Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;
- What damages Plaintiffs and Class Members suffered because of Defendant's misconduct;
- Whether Defendant's conduct was negligent;
- Whether Defendant breached contracts it had with its clients, which were made expressly for the benefit of Plaintiffs and Class Members;
- Whether Plaintiffs and Class Members are entitled to damages;
- Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and among other things,
- Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

142. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

143. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel are competent and experienced in

litigating class actions, including data privacy litigation of this kind.

144. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

145. Superiority. A class action is superior to other available methods 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. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating her individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

146. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

147. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data

Breach, as is evident by Defendant's ability to send those individuals notification letters.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

148. Plaintiffs repeat and reincorporate paragraphs 1-147 of this Compliant, as if fully set forth herein.

149. Plaintiffs and Class Members provided their non-public Private Information to Defendant as a condition of financial services.

150. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

151. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

152. Defendant had duties to employ reasonable security measures in accordance with the standard of care, which in part is established under Section 5 of the FTCA, 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 confidential data.

153. Defendant's duty to use reasonable security measures in compliance with the standard of care arose under the common law, and as informed by the FTC Act and the HIPAA Security Rule, which mandates that Defendant implement reasonable cybersecurity measures.

154. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

155. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

156. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and 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 is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

157. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- Allowing unauthorized access to Class Members' Private Information;
- Failing to remove Plaintiffs' and Class Members' Private Information it was no longer required to retain pursuant to regulations; and
- Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

158. Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

159. Defendant's violation of the FTC Act and HIPAA also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiffs and the proposed Class Members from the harms associated with data breaches.

160. Defendant has admitted that the Private Information of Plaintiffs and Class Members was lost and disclosed to unauthorized third persons because of the Data Breach.

161. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

162. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

163. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal

damages; and (viii) the continued and certainly increased risk to their PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) 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 Private Information.

164. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs 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.

165. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

166. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

167. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendant's decision not to invest enough resources in its cyber defenses amounts to gross negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs repeat and reincorporate paragraphs 1-147 of this Compliant, as if fully set forth herein.

169. Plaintiffs and the proposed Class Members transferred their Private Information to Defendant as part of receiving services.

170. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiffs and Class Members and implicitly agreed to do so.

171. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as a necessary part of receiving services.

172. Defendant, however, failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

173. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PHI, they would not have allowed it to be provided to Defendant.

174. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) 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 Private

Information.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

175. Plaintiffs repeat and reincorporate paragraphs 1-147 of this Compliant, as if fully set forth herein.

176. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

177. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information provided to Defendant, along with payment, as a condition of receiving services.

178. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members.

179. Because of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the value of services with reasonable data privacy and security practices and procedures, and the services without unreasonable data privacy and security practices and procedures that they received.

180. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the proposed Class Members' monies paid and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiffs and the Class Members would not have provided their Private Information, nor paid Defendant, had they known Defendant would not adequately protect their Private Information.

181. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it because of their

misconduct and the Data Breach alleged herein.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs repeat and reincorporate paragraphs 1-147 of this Compliant, as if fully set forth herein.

183. Plaintiffs and Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public.

184. Plaintiffs' and Class Members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the public prior to the Data Breach.

185. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

186. Defendant owed a duty to its patients, including Plaintiffs and the proposed Class Members, to keep their Private Information confidential.

187. The unauthorized release of Private Information is highly offensive to any reasonable person.

188. Plaintiffs' and Class Members' Private Information is not of legitimate concern to the public.

189. Defendant knew or should have known that Plaintiffs' and Class Members' Private Information was private.

190. Defendant publicized Plaintiffs' and Class Members' Private Information, by communicating it to cybercriminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information by injecting it into the illicit stream of commerce flowing through the dark web and other malicious channels of communication (e.g.,

Telegram and Signal).

191. It is therefore likely that the Plaintiffs' and the Class Members' Private Information is rapidly becoming public knowledge–among the community writ large–due to the nature of the malware attack that procured it, and the identity theft that it is designed for.

192. Moreover, because of the ubiquitous nature of data breaches, especially in the healthcare industry, Defendant was substantially certain that a failure to protect Private Information would lead to its disclosure to unauthorized third parties, including the thousands of waiting identity thieves who are in a special relationship to Plaintiffs and the proposed Class Members—in that those identity thieves are precisely the individuals whose aim it is to misuse such Private Information.

193. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that Defendant's inadequate data security measures will likely result in additional data breaches. Plaintiffs and Class Members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiffs' and Class Members' privacy by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and

Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and

audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

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

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

x. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xi. requiring Defendant to implement a system of tests to assess its

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xiv. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: August 14, 2025

Respectfully submitted,

/s/ Jon Mann

Jonathan S. Mann (MAN057)
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
jonm@pittmandutton.com

J. Gerard Stranch, IV (*pro hac vice*)
STRANCH, JENNINGS, & GARVEY, PLLC
223 Rosa Parks Ave. Suite 200
Nashville, TN 37203
Tel: 615/254-8801
gstranch@stranchlaw.com

Mariya Weekes (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200
mweekes@milberg.com

Interim Co-Lead Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that on August 14, 2025, I electronically filed the foregoing with the Clerk of Court using the AlaFile system, which will send notification of such filing to all counsel of record.

Josh Becker
Jonathan R. Hirsch
Shook, Hardy & Bacon L.L.P.
1230 Peachtree Street NE, Suite 1200
Atlanta, GA 30309
Tel: (470) 867-6000
jbecker@shb.com
jhirsch@shb.com

Attorneys for Defendant AOD Federal Credit Union

/s/ Jon Mann
Of Counsel