UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA

SHERRY NEFF, KELLY MCCOLLUM, and CARLOS RIVERA, individually and on behalf of all others similarly situated, Plaintiffs, v. MCBS, LLC, Defendant.	Case No. 1:25-cv-00235 JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

1. Plaintiff Sherry Neff, Kelly McCollum, and Carlos Rivera ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Amended Class Action Complaint against Defendant MCBS, LLC ("MCBS" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

2. This class action arises out of Defendant MCBS's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes. This failure to secure and monitor its network resulted in a September 2025 data breach ("Data Breach") of highly sensitive documents and information stored on the computer network of MCBS, an organization that provides medical billing and/or employment to individuals, including Plaintiffs and Class Members.

3. Defendant's data security failures allowed a targeted cyberattack in or about September 2025 to compromise Defendant's network (the "Data Breach") that contained personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiffs and other individuals ("the Class").

4. Upon information and belief, on or about September 25, 2025, the threat actor "PEAR" successfully breached MCBS's inadequately protected computer systems and accessed and exfiltrated an unknown quantity of highly sensitive data. The incident was publicly reported on BreachSense. As of the filing of this Amended Complaint, Defendant has not provided any kind of notice to affected individuals. [1]

5. PEAR ransomware is one of the most active ransomware groups targeting US entities in 2025 and is known for its rapid, professional attacks against healthcare and other American organizations. The group gains access mainly by using stolen or purchased VPN or RDP credentials, or by exploiting vulnerabilities through weak company data protection policies, and quickly exfiltrates data before deploying file-encrypting malware. [2]

6. The types of information that PEAR has routinely exfiltrated in their ransomware attacks include, but are not limited to: names, birthdates, addresses, Social Security numbers, health insurance details, medical treatment data, financial records, intellectual property, accounting documents, legal files, personnel and customer information, banking details, etc.

7. The information collected at MCBS in order to receive medical services or employment included certain personal or protected health information of current and former

[1] Breachsense, "Data breach and dark web monitoring tool," https://www.breachsense.com/breaches/mcbs-data-breach/ (last visited Nov. 19, 2025).
[2]https://www.hookphish.com/blog/ransomware-group-pear-hits-mcbs-llc/(last visited Nov. 18, 2025).

employees and patients, including Plaintiffs. This Private Information, stored on Defendant's computer network, included, but is not limited to: names, addresses, dates of birth, email addresses, Social Security numbers, government identification information/driver's license numbers/ passport numbers, health insurance providers, medical treatment information, medical diagnoses, medications, and lab results.

8. Upon information and belief, the cybercriminals intentionally targeted MCBS for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive Private Information, including but not limited to Social Security numbers. As a result, the Private Information of Plaintiffs and Class remains in the hands of those cyber-criminals.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for either treatment or employment or both.

10. Plaintiffs bring this class action lawsuit on behalf of themselves, and all others 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 Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and including in that notice precisely what specific types of information were accessed and taken by cybercriminals.

11. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant MCBS's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a

known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice—or any notice at all— of the Data Breach.

13. In addition, Defendant MCBS failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its systems, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the Private Information of Plaintiffs Class Members.

14. Plaintiffs and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant MCBS collected and maintained is now in the hands of data thieves.

15. Armed with the Private Information accessed in the Data Breach, data thieves can 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, filing false medical claims 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.

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

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

18. Through this Amended Complaint, Plaintiffs seek to remedy these harms on behalf of themselves, and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

19. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; and (v) unjust enrichment, and (vi) declaratory relief.

20. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

21. Plaintiff Sherry Neff is and at all times mentioned herein was an individual citizen of Salisbury, , and is a patient whose healthcare providers utilize MCBS for medical billing and reimbursement services.

22. Plaintiff Kelly McCollum is and at all times mentioned herein was an individual citizen of Raytown, Missouri, and, is a patient whose healthcare providers utilize MCBS for medical billing and reimbursement services.

23. Plaintiff Carlos Rivera is and at all times mentioned herein was an individual citizen of Grand Island, Florida, and is a patient whose healthcare providers utilize MCBS for medical billing and reimbursement services.

24. MCBS, LLC is a Georgia medical billing practice that has its principal place of business at 1125 Troupe Street, Augusta, Georgia 30904. It can be served through its registered agent, at its principal place of business.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant, including Plaintiffs.

26. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a corporation; it maintains its headquarters in Georgia; and it committed tortious acts in Georgia.

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which MCBS is headquartered and has the most significant contacts.

FACTUAL ALLEGATIONS

Defendant's Business

28. Defendant MCBS claims to be the "…the solution! With over 35 years of experience in the Medical Billing Industry."[3]

29. MCBS has one location that offers services such as practice management and accounts receivable management. [4]

30. In the ordinary course of receiving third party medical billing services from Defendant MCBS, or alternatively being employed by MCBS, each patient (through its medical provider) and employee must provide (and Plaintiffs did provide) Defendant MCBS with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and

[3] https://www.mcbs.com/#/index.cfm (last visited Nov. 18, 2025).
[4] *Id.*

- Banking and/or credit card information.

31. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

32. Upon information and belief, Defendant MCBS LLC, acting as a business associate to various medical providers, is responsible for administering billing services that require the receipt, storage, and handling of patients' Protected Health Information ("PHI"). Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"), 45 C.F.R. §§ 160 and 164, MCBS LLC is required to adopt and maintain adequate privacy and security practices to protect patient PHI.

33. Defendant MCBS had a legal duty to ensure that PHI provided by Plaintiffs and Class Members was maintained in a secure, confidential manner and in compliance with HIPAA, the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and other applicable laws. Through its agreements with covered entities, Defendant MCBS LLC also undertook contractual obligations to safeguard PHI and follow HIPAA-required procedures, including providing access to a compliant Notice of Privacy Practices.

34. Despite these obligations, MCBS failed to post, provide, or make available any HIPAA-compliant privacy policy on its publicly accessible website, thereby depriving patients of critical information about how their PHI would be collected, used, and protected. Moreover, as alleged herein, Defendant failed to implement appropriate administrative, technical, and physical safeguards to adequately protect PHI, causing Plaintiffs and Class Members' sensitive medical and personal information to be exposed.

35. The Private Information at issue includes, but is not limited to, Plaintiffs and Class Members' names, addresses, Social Security numbers, dates of birth, medical billing records,

insurance information, and other sensitive identifiers. By failing to properly secure this information, MCBS violated HIPAA, reneged on its legal obligations, and failed to meet the assurances inherent in its role as a business associate entrusted with the PHI of thousands of patients.

The Data Breach

36. A data breach occurs when cybercriminals access or steal Private Information that has not been adequately secured by a business entity like MCBS.

37. Upon information and belief, Defendant experienced a cyberattack on its computer systems by threat actor PEAR on or around September 25, 2025, when it took many of the business's networked systems offline, adversely affecting medical billing services, and stole Plaintiffs' and Class Members' Private Information.[5]

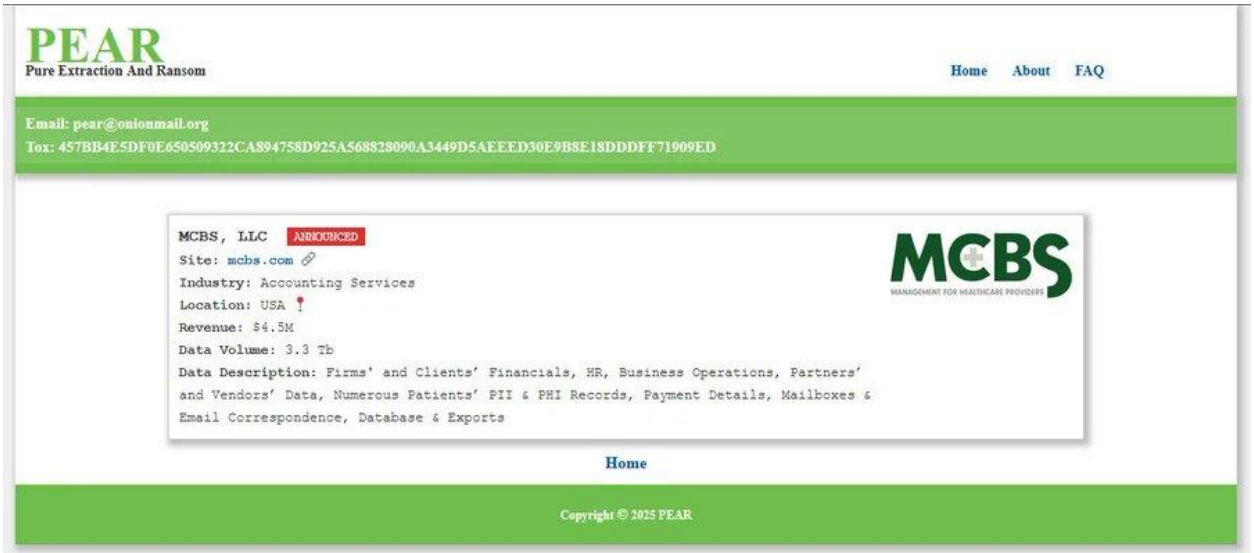
38. PEAR is a notorious ransomware group known for a "double extortion" strategy involving both data encryption and the threat of public exposure of stolen sensitive information.[6] The group first emerged publicly around mid-2025 and has targeted a variety of sectors, particularly in the United States, including healthcare, accounting, law firms, and manufacturing.[7]

39. PEAR claims to have exfiltrated 3.3 TB of data taken from Defendant's inadequate computer systems, including files containing highly sensitive Private Information, and has posted about the Data Breach on the dark web.[8]

---

[5] https://undercodenews.com/massive-ransomware-attacks-shake-us-companies-azpro-group-and-mcbs-llc-targeted/ (last visited Nov. 18, 2025).
[6] https://digitalrecovery.com/en/decrypt-ransomware/pear/#:~:text=PEAR%20ransomware%20is%20an%20advanced,additional%20pressure%20tactic%20on%20victims. (last visited Nov. 18, 2025).
[7] *Id.*
[8] https://dailydarkweb.net/mcbs-llc-hit-by-pear-ransomware-in-significant-data-breach/ (last visited Nov. 18, 2025).

40. As shown below and upon information and belief, PEAR disclosed the Data Breach on the dark web and made the Private Information publicly available for sale, including Plaintiffs' and Class Members' PII and PHI records, payment details, mailboxes, email correspondence, and more. [9]



41. Upon information and belief, Defendant had failed negotiations with PEAR, which would have required them to pay a ransom of the exfiltrated data to prevent PEAR from further disseminating the Private Information on the dark web.[10]

42. Defendant has yet to notify HHS of the Data Breach that occurred on or about September 25, 2025.

43. As of the filing of this Amended Complaint, upon information and belief, the required State Attorney Generals' notices have not been sent, nor have patients and employees received direct notice of whether their Private Information was breached and exfiltrated.

[9] *Id.*
[10] *Id.*

44. In January 2023, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendant, of the severe threats posed by cybercriminal groups, similar to PEAR.[11] Within the healthcare industry, the risk of a cyber-attack is well-known and preventable with adequate security systems in place.

45. MCBS's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

46. MCBS knew or should have known that its electronic records would be targeted by cybercriminals.

47. MCBS had obligations created by HIPAA, FTCA, contract, industry standards, common law, state law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice.

49. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including MCBS, are well-aware of the risk of being targeted by cybercriminals.

50. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

[11] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last visited Nov. 18, 2025).

51. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss." [12]

52. Individuals, like Plaintiffs and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

53. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

54. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other government agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee

[12] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited Nov. 18, 2025).

you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[13]

55. In 2024, there were a record 3,158 data breaches, similar to the 3,202 breaches reported in 2013. Furthermore, the number of victims affected jumped to 1.73 billion people, which is a 300% increase from 2024 to 2023.[14]

56. Additionally, "in 2024, healthcare data breaches reached an all-time high, with 276,775,457 records compromised – a 64.1% increase from the previous year's record and equivalent to 81.38% of the United States population." In a new report issued, "more than 2,400 security leaders and found that the top predicted threat for 2025 is ransomware. According to the report, nearly 1 out of every 3 security professionals (38%) believe ransomware will become an even greater threat when powered by AI." This is particularly alarming as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from businesses "lack of cybersecurity expertise and significant security resources."[15]

57. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

58. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations

[13] https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 18, 2025).
[14] https://www.cnet.com/tech/services-and-software/near-record-number-of-data-breaches-reported-in-2024-report-says/ (last visited Nov. 18, 2025).
[15] https://www.forbes.com/sites/chuckbrooks/2025/04/05/key-cybersecurity-challenges-in-2025-trends-and-observations/ (last visited Nov. 18, 2025).

and the loss of critical information and data." [16] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[17]

59. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, MCBS failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

60. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

61. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[18]

62. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health

[16] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited Nov. 18, 2025).
[17] *Id.*
[18] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited Nov. 18, 2025).

insurance information, and medical and clinical data, and that information can be easily monetized."[19]

63. The HIPAA Journal article goes on to explain that patient records, like those stolen from MCBS, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[20]

64. Data breaches such as the one experienced by Defendant MCBS have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

65. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[21]

66. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[22]

67. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In

---

[19] *Id.*
[20] *Id.*
[21] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Nov. 18, 2025).
[22] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last visited Nov. 18, 2025).

fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[23]

68. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant MCBS.

Defendant Fails to Comply with FTC Guidelines.

69. The Federal Trade Commission ("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.

70. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that 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.[24] 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 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.[25]

---

[23] https://www.ahu.edu/blog/data-security-in-healthcare (last visited Nov. 18, 2025).
[24] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 18, 2025).
[25] *Id*.

71. 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

72. The FTC has brought enforcement actions against businesses, like that of MCBS, for failing to adequately and reasonably protect patient 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

74. Defendant failed to properly implement basic data security practices.

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards.

77. As shown above, experts studying cybersecurity routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

78. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

79. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

80. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both 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).

81. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Defendant's Conduct Violates HIPAA.

82. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

83. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

84. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

85. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

86. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant has Breached its Obligations to Plaintiffs and Class.

87. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and its patients' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

88. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiffs and Class Members' Private Information.

89. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identity Theft.

90. Data Breaches such as the one experienced by Plaintiffs and the Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

91. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[26] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiffs and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

92. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report"). [27]

93. The FTC, like the GAO (*see* Exhibit A), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting

[26] https://www.gao.gov/assets/gao-19-230.pdf (last visited Nov. 18, 2025).
[27] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Nov. 18, 2025). ("2007 GAO Report").

companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[28]

94. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

95. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

96. Theft of Private Information is also gravely serious. Private Information is a valuable property right.[29]

97. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies 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.

See 2007 GAO Report, at p. 29.

[28] *See* https://www.identitytheft.gov/Steps (last visited Nov. 18, 2025).
[29] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

98. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

99. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

100. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[30]

101. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[31] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[32] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's

[30] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last visited Nov. 18, 2025).
[31] *Identity Theft and Your Social Security Number*, Social Security Administration (last visited Nov. 18, 2025).(2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 18, 2025).
[32] *Id.* at 4.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

102. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he 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."[33]

103. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[34]

104. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFFS' EXPERIENCES

[33] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Nov. 18, 2025).
[34] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 18, 2025).

Plaintiff Sherry Neff

105. Plaintiff Sherry Neff is and at all times mentioned herein was an individual citizen residing in the State of Maryland.

106. Plaintiff Neff is a patient whose healthcare providers utilize MCBS for medical billing and reimbursement services, and entrusted MCBS with highly sensitive Private Information, including but not limited to: full name, date of birth, Social Security number, insurance information, protected health information, financial account information, driver's license, and home addresses. Upon information and belief, this Private Information was maintained on MCBS's computer systems on or around September 25, 2025, when those systems were subject to unauthorized access and exfiltration by cybercriminals. Plaintiff Neff's Private Information, therefore, was among the data compromised in the incident.

107. Following the Data Breach, Plaintiff Neff became aware of the incident through her own online research after receiving a notification that her information has been leaked on the dark web.

108. Since the Data Breach, Plaintiff Neff monitors her financial accounts for about 2 hours per week. This is more time than she spent prior to learning about the MCBS's Data Breach. Having to do this every week not only wastes her time as a result of MCBS's negligence, but it also causes her great anxiety.

109. Since the Data Breach, Plaintiff Neff began receiving an excessive number of spam calls on the same cell phone number provided to MCBS on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen Private Information.

110. Since the Data Breach, Plaintiff Neff has also begun receiving a high volume of spam and phishing emails sent to the same email address she provided to MCBS as part of her patient records. These emails are persistent, time-consuming to delete, and often appear designed to obtain additional personal or financial information. Given the timing and similarity to the surge in spam calls, Plaintiff Neff reasonably believes that the influx of emails is related to the compromise of her Private Information in the Data Breach.

111. On September 29, 2025, after the Data Breach occurred, Plaintiff Neff received a fraud alert from her bank notifying her of an attempted unauthorized check made using her financial account information. As a result, Plaintiff Neff was required to replace her debit cards to secure her account. Plaintiff Neff had never previously experienced fraudulent activity of this kind and, given the close timing to the Data Breach, reasonably believes this incident was a direct result of Defendant's failure to safeguard her Private Information.

112. Since learning of the Data Breach, Plaintiff Neff has proactively changed all of her online account passwords. Out of concern for future fraud or unauthorized charges, she has also refrained from linking her new banking card to the accounts that automatically bill through her bank. Plaintiff's actions reflect her ongoing fear and anxiety about the continued misuse of her Private Information resulting from the Data Breach.

113. Plaintiff Neff is aware that cybercriminals often sell Private Information, and once stolen, their Private Information is likely to be abused months or even years after MCBS's Data Breach.

114. Had Plaintiff Neff been aware that MCBS's computer systems were not secure, she would not have entrusted MCBS with her Private Information.

Plaintiff Kelly McCollum

115. Plaintiff Kelly McCollum is and at all times mentioned herein was an individual citizen residing in the State of Missouri.

116. Plaintiff McCollum is a patient whose healthcare providers utilize MCBS for medical billing and reimbursement services, and entrusted MCBS with highly sensitive Private Information, including but not limited to: full name, date of birth, Social Security number, insurance information, protected health information, financial account information, driver's license, and home addresses.

117. Upon information and belief, this Private Information was maintained on MCBS's computer systems on or around September 25, 2025, when those systems were subject to unauthorized access and exfiltration by cybercriminals. Plaintiff McCollum's Private Information, therefore, was among the data compromised in the incident.

118. Following the Data Breach, Plaintiff McCollum became aware of the incident through her own online research after receiving a notification that her information has been leaked on the dark web on October 3, 2025.

119. Since the Data Breach, Plaintiff McCollum monitors her financial accounts for about 4-5 hours per week. This is more time than she spent prior to learning about the MCBS's Data Breach. Having to do this every week not only wastes her time as a result of MCBS's negligence, but it also causes her great anxiety.

120. Since learning of the Data Breach, out of concern for future fraud or unauthorized charges, she has also replaced her banking cards. Plaintiff McCollum's actions reflect her ongoing fear and anxiety about the continued misuse of her Private Information resulting from the Data Breach.

121. Plaintiff McCollum is aware that cybercriminals often sell Private Information, , and once stolen, their Private Information is likely to be abused months or even years after MCBS's Data Breach.

122. Had Plaintiff McCollum been aware that MCBS's computer systems were not secure, she would not have entrusted MCBS with her Private Information.

Plaintiff Carlos Rivera

123. Plaintiff Carlos Rivera is and at all times mentioned herein was an individual citizen residing in the State of Florida.

124. Upon information and belief, Plaintiff Rivera is a patient whose healthcare providers utilize MCBS for medical billing and reimbursement services, and entrusted MCBS with highly sensitive Private Information, including but not limited to: full name, date of birth, Social Security number, insurance information, protected health information, financial account information, driver's license, and home addresses.

125. Upon information and belief, this Private Information was maintained on MCBS's computer systems on or around September 25, 2025, when those systems were subject to unauthorized access and exfiltration by cybercriminals. Plaintiff Rivera's Private Information, therefore, was among the data compromised in the incident.

126. Following the Data Breach, Plaintiff Rivera became aware of the incident through his own online research.

127. Since the Data Breach, Plaintiff Rivera monitors his financial accounts routinely. This is more time than he spent prior to learning about the MCBS's Data Breach.

128. Since the Data Breach, Plaintiff Rivera began receiving an uptick in spam calls on the same cell phone number provided to MCBS on his records.

129. Since the Data Breach, Plaintiff Rivera has also begun receiving a high volume of spam and phishing emails sent to the same email address he provided to MCBS as part of his patient records. These emails are persistent, time-consuming to delete, and often appear designed to obtain additional personal or financial information. Given the timing and similarity to the surge in spam calls, Plaintiff Rivera reasonably believes that the influx of emails is related to the compromise of his Private Information in the Data Breach.

130. Plaintiff Rivera is aware that cybercriminals often sell Private Information, and once stolen, their Private Information is likely to be abused months or even years after MCBS's Data Breach.

131. Had Plaintiff Rivera been aware that MCBS's computer systems were not secure, he would not have entrusted MCBS with his PII and PHI.

PLAINTIFFS' AND CLASS MEMBERS' INJURIES

132. To date, Defendant MCBS has done absolutely nothing to compensate Plaintiffs and Class Members for the damages they sustained in the Data Breach.

133. Defendant MCBS has yet to offer credit monitoring services, which is inadequate when victims are likely to face many years of identity theft.

134. MCBS's lack of offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs and Class Members' Private Information, out-of-pocket costs, and the time they are required to spend attempting to mitigate their injuries.

135. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

136. Plaintiffs' and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

137. Plaintiffs and Class were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

138. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

139. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

140. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

141. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

142. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

143. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

144. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing “freezes” and “alerts” with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

145. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

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

147. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, MCBS knew of the breach ***since September 30, 2025*** and has not yet notified victims. Yet MCBS offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiffs and Class.

CLASS ACTION ALLEGATIONS

148. Plaintiffs bring this action on behalf of themselves, and on behalf of all other persons similarly situated.

149. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach discovered by MCBS, LLC. in September 2025 (the "Class").

150. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

151. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

152. Numerosity, The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs at this time, but the number class members are believed to be in the thousands.

153. 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:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

154. Typicality, Plaintiffs claims are typical of those of other Class Members because Plaintiffs Private Information, like that of every other Class member, were compromised in the Data Breach.

155. Adequacy of Representation, Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

156. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs and Class Members' data was stored on the same computer systems and unlawfully accessed 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.

157. Superiority, A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their 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, the conduct of 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.

158. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

159. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach;

g. Whether Defendant failed to abide by its responsibilities under HIPAA.

160. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiffs and Class Members)

161. Plaintiffs incorporate by reference all allegations in paragraphs 1-160 as if fully set forth herein.

162. Defendant MCBS required Plaintiffs and Class Members to submit non-public PII and PHI in order to obtain healthcare/medical services and/or employment, and Defendant owed various duties of care pursuant to common law, industry standards, and statutory law.

163. By collecting and storing this data in MCBS's computer systems, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

164. 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.

165. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant also had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

166. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant MCBS and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant

was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

167. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

168. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

169. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

170. Defendant breached its duties, and thus were 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:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

171. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

172. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

173. Plaintiffs and Class Members have been injured by Defendant's negligent actions alleged herein and are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

174. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

175. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Second Count
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

176. Plaintiffs incorporate by reference the allegations in paragraphs 1-160 as if fully set forth herein.

177. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

178. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Private Information.

179. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

180. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, and adequate data security practices to safeguard Plaintiffs and Class Members' Private Information.

181. Defendant's failure to comply with applicable laws and regulations, including the FTC Act and HIPAA, constitutes negligence *per se.*

182. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

183. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause Plaintiffs and Class

Members to experience the foreseeable harms associated with the exposure of their Private Information.

184. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Third Count
Breach of Implied Contract
(On Behalf of Plaintiffs and Class Members)

185. Plaintiffs incorporate by reference the allegations in paragraphs 1-160 as if fully set forth herein.

186. Plaintiffs and Class Members provided their Private Information to Defendant MCBS in exchange for Defendant's medical billings services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

187. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

188. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

189. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

190. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

191. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

192. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

193. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

194. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

195. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

196. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class Members.

Fourth Count
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and Class Members)

197. Plaintiffs incorporate by reference the allegations in paragraphs 1-160 as if fully set forth herein.

198. Plaintiffs are each medical patients whose medical providers used MCBS's medical billing services in providing care to Plaintiffs.

199. As the business associate and agent of its healthcare clients, and the recipient of Plaintiffs' and Class Members' Private Information, MCBS has a fiduciary relationship with Plaintiffs and Class Members.

200. Defendant became the guardian of Plaintiffs and Class Members' Private Information as the business associate and agent of medical providers; therefore, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Private Information; (2) to timely notify Plaintiffs 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.

201. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Private Information.

202. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give any notice of the Data Breach to Plaintiffs and Class in a reasonable and practicable period of time.

203. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Private Information.

204. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

205. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Private Information.

206. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) 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; (v) the continued risk to their Private 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 Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

207. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

Fifth Count
Unjust Enrichment
(On Behalf of Plaintiffs and Class Members)

208. Plaintiffs incorporate by reference the allegations in paragraphs 1-160 as if fully set forth herein.

209. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

210. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

211. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

212. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

213. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

214. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

215. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

216. Defendant failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

217. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

218. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

219. Plaintiffs and Class Members have no adequate remedy at law.

220. 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: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their Private 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 Private Information in their

continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

222. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

Sixth Count
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and Class Members)

223. Plaintiffs incorporate by reference the allegations in paragraphs 1-160 as if fully set forth herein.

224. Plaintiffs and Class Members are third-party beneficiaries of contracts entered into between their healthcare providers and MCBS, under which MCBS received Plaintiffs' and Class Members' Private Information, stored that information in its computer network systems, and provided medical billing and other services to Plaintiffs' and Class Members' healthcare providers, MCBS's customers.

225. Upon information and belief, all of MCBS's contracts with its healthcare provider clients, including Plaintiffs' and Class Members' healthcare providers, obligated MCBS to implement and maintain reasonable, industry-standard, HIPAA-compliant measures to protect the Private Information MCBS received, used, and stored in the course of performing these contracts from unauthorized disclosure.

226. Plaintiffs and Class Members, as patients of healthcare providers that contracted with MCBS, were the intended beneficiaries of MCBS's contractual obligations with respect to data security, in that these obligations were expressly undertaken for the protection of MCBS's clients' patients' Private Information.

227. MCBS breached the foregoing contracts by failing to adequately protect Plaintiffs' and the Class Members' Private Information in accordance with its contractual obligations, causing its unauthorized access, exposure, and theft in the Data Breach, and Plaintiffs' and Class Members' attendant injuries and damages.

228. As a direct and proximate result of MCBS's breach of third-party beneficiary contract, Plaintiff and Class Members are entitled to actual, compensatory, and consequential damages, in an amount to be determined at trial.

Seventh Count
Declaratory Judgment
(On Behalf of Plaintiffs and Class Members)

229. Plaintiffs incorporate by reference the allegations in paragraphs 1-160 as if fully set forth herein.

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

231. An actual controversy has arisen in the wake of the Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security

measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information.

232. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs will continue to suffer injury because of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

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

a. Defendant continues to owe a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law, state law, HIPAA, Section 5 of the FTC Act, and various states' statutes; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

234. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

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

236. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiff sand Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

237. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the thousands of individuals whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their 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 equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, nominal damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

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

h) Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

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

Dated: November 20, 2025

Respectfully submitted,

/s/ Andrew J. Shamis
Andrew J. Shamis (GA Bar No. 494196)
SHAMIS & GENTILE, P.A.
26 Grand Georgian Ct
Cartersville, GA 30121
Telephone: 305-479-2299
ashamis@shamisgentile.com

Gary E. Mason (*pro hac vice forthcoming)*
Danielle L. Perry (*pro hac vice forthcoming*)
MASON LLP
5335 Wisconsin Avenue NW, Ste. 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com

Email: dperry@masonllp.com

Joshua Gordon Schiffer
JD LAW GROUP
912 Holcomb Bridge Road
Suite 203
Roswell, GA 30326
404-842-0909
Fax: 404-719-4273
Email: Josh@csfirm.com

Casondra Turner (GA Bar No. 418426)
MILBERG, PLLC
260 Peachtree Street, NW
Suite 2200
Atlanta, Georgia 30303
Tel: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on November 20, 2025, the foregoing Amended Class Action Complaint was filed using CM/ECF, which will send service of same to all counsel of record.

/s/ Andrew J. Shamis
Andrew J. Shamis